Spring 2003

ACUTA Journal of Telecommunications in Higher Education

Spring, 2003
Vol.7, No.1

ACUTA

Journal

of Communications Technology in Higher Education

Published by The Association for Communications Technology Professionals in Higher Education

This Issue: Disaster Preparedness and Business Continuity

Spring Seminars

April 27–30, 2003
Norfolk, Va.
Sheraton Norfolk Waterside

I. Wireless Technologies

Track I will focus on Wireless Technologies, looking at regulatory issues, trends in wireless standards and products, engineering wireless coverage, carrier negotiations, revenue from cellular, trends in student use of cell phones, developing building access agreements, and funding deployment of wireless data systems.

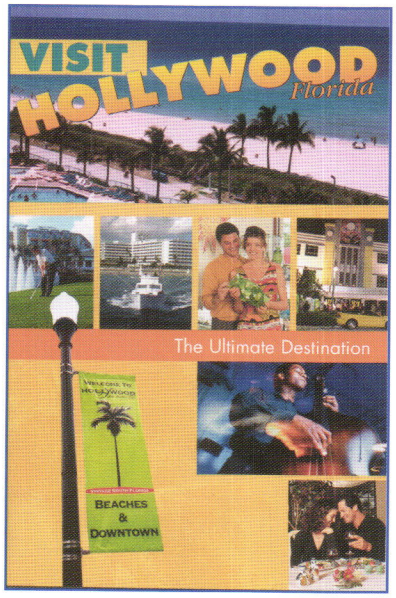
II. Regulatory Update

Track II will focus on Regulatory Issues including wireless issues, IP telephony access charges, Universal Service, consumer issues, challenges to long-distance contracts, 271 long-distance approvals for CLECs, unauthorized charges, strategies for negotiating with carriers, building access and service level agreements.

ACUTA
The Association for Communications Technology Professionals in Higher Education
152 W. Zandale Dr., Ste. 200
Lexington, KY 40503-2486
859/278-3338

For more details or to register online, visit our Web site at www.acuta.org

32nd Annual Conference & Exhibition



July 27–31, 2003 · Hollywood, Fla.
Westin Diplomat Resort & Spa

- ★ Opportunities to network with hundreds of your peers from campuses coast to coast
- ★ Keynote Speakers: Bruce Jenner, Larry Irving, Jeff Linder, Tom Ryan
- ★ 50+ breakout sessions on subjects such as network security, wireless, disaster recovery, universal service, IT funding, VoIP
- ★ 80+ vendors in the Exhibit Hall, ready to discuss new products and services. You might win some terrific prizes!
- ★ Awards presentations, user groups, and a variety of social events to promote interaction among attendees

Conference within a Conference

The ACUTA Forum for Strategic Leadership in Communications Technology: July 28-29, 2003

"Strategies for Management in a Difficult Economy"

The Strategic Leadership Forum is a unique opportunity for leaders who are responsible for planning and implementing communications and information technology to learn from the experiences and expertise of senior higher-education leaders and their peers. This year, we have invited Presidents, Chief Business Officers, Advancement Officers, and CIOs to share their perspectives on technology in an era of reduced budgets and increased expectations.

Who Should Attend? Anyone with senior strategic-planning and decision-making responsibility for communications and/or information technology.

Interested? Contact Lori Dodson at ACUTA, ldodson@acuta.org, and we will put your name on the Strategic Leadership Forum mailing list.

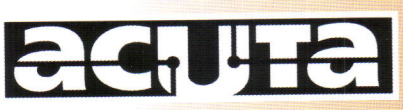
Events Calendar

Event	Date	Place
Spring Seminars	April 27–30, 2003	Sheraton Norfolk Waterside Norfolk, Virginia
Annual Conference	July 27–31, 2003	The Westin Diplomat Resort and Spa Hollywood, Florida
Fall Seminars	October 19–22, 2003	Hilton San Diego Resort San Diego, California
Winter Seminars	January 11–14, 2004	Sheraton New Orleans New Orleans, Louisiana

ACUTA's Core Purpose is to: Support higher education institutions in achieving optimal use of communications technologies.

ACUTA's Core Values are to:

- Share information, resources and insight,
- Respect the expression of individual opinions and solutions,
- Maintain our commitment to professional development and growth,
- Advance the unique values and needs of higher education communications technologies, and
- Encourage volunteerism and individual contribution of members in support of organizational goals.



"Any campus that hasn't put a great deal of thought and planning into how it would respond in a crisis is courting disaster."

Ron Walczak
page 11

THE ACUTA JOURNAL OF TELECOMMUNICATIONS IN HIGHER EDUCATION

Published Quarterly by
ACUTA: The Association for Communications Technology Professionals in Higher Education
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486

PHONE 859/278-3338
FAX 859/278-3268
E-MAIL pscott@acuta.org

Publisher
Jeri A. Semer, CAE, Executive Director

Editor-in-Chief
Pat Scott, Communications Manager

Contributing Editor
Curt Harler

Advertising Sales
KCS International, LLC
717/397-7100 or www.kcsinternational.com

Submissions Policy
The ACUTA Journal welcomes submissions of editorial material. We reserve the right to reject submissions or to edit for grammar, length, and clarity. Send all materials or letter of inquiry to Pat Scott, Editor-in-chief. Author's guidelines are available upon request or online at www.acuta.org.

The opinions expressed in this publication are those of the writers and are not necessarily the opinions of their institution or company. ACUTA, as an association, does not express an opinion or endorse products or services.

The ACUTA Journal is published four times per year by ACUTA, a nonprofit association for institutions of higher education, represented by telecommunications managers and staff.

ISSN 1097-8658

POSTMASTER, send all address changes to:

ACUTA
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486
Postage paid at Louisville, Kentucky.

Visit the ACUTA site on the World Wide Web:
http://www.acuta.org

Membership and Subscriptions
Subscriptions are provided as a benefit of membership. The publication is available to nonmembers for $80 per year or $20 per issue. For information, contact Kellie Bowman, Membership Development Manager, 859/278-3338, ext. 222, or e-mail, kbowman@acuta.org.

Contents

Spring 2003 • Volume 7, Number 1
Disaster Preparedness and Business Continuity

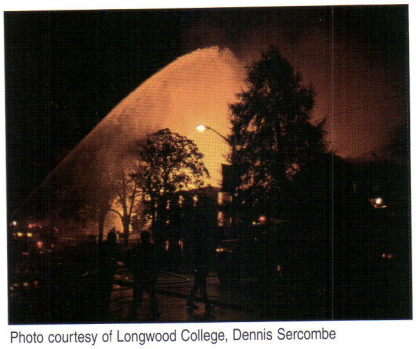


Photo courtesy of Longwood College, Dennis Sercombe

FEATURES

INTERVIEW

COLUMNS

LEADERSHIP AWARD

ADVERTISERS' INDEX

PRESIDENT'S MESSAGE

Planning for Disasters in 2003

Jeanne Jansenius
University of the South
ACUTA President
2002–2003

In most higher-education institutions, disaster plans include recovery from events such as floods, HVAC outages, power outages, fires, earthquakes, and lightning strikes. Since September 11, 2001, those who formulate responses to disasters have expanded those plans to include total destruction recovery, security breaches, and potential hostage situations. There is a growing sense of urgency to make certain that our campuses are prepared to respond to a wider variety of situations than ever before, and most plans include testing to ensure the continuity of operations and availability of critical resources. Among the key elements of the planning process are minimizing the disruption of operations, ensuring organizational stability, and implementing an orderly recovery process.

With its focus on learning and experimentation, the higher-education environment has always been rather decentralized and open-ended. Campus security and safety officers are now insisting that institutions increase their overall security.

Michael Zastrocky, from Gartner, Inc., stated at the ACUTA 2003 Winter Seminar, "Every member of the campus community must be aware of and accountable for security policy, procedure, and consequences." A disaster may affect only one building, or it might have an impact on the whole campus. A disaster may involve the mobilization of only a few responders, or it may involve assistance from outside agencies. It is important that everyone on campus take ownership of his or her areas of responsibility during a disaster.

It is also important that every institution understand and be aware of its environment and anticipate what might happen. Try to identify who might want to cause your institution harm. At the seminar in January, Steven Hailey, with DayCom Systems, Inc., advised that "the primary objective of a disaster recovery plan is to enable an organization to survive a disaster and to continue normal business operations. In order to survive, the organization must assure that critical operations can resume/continue normal processing. Throughout the recovery effort, the plan establishes clear lines of authority and prioritizes work efforts." (http://www.acuta.org/relation/downloadfile.cfm?DocNum=688)

Some essential directives in a disaster preparedness and business continuity plan include the following:

- Prepare for a total loss; this will minimize risk of delays.
- Provide for the safety and well being of people on the premises at the time of a disaster.
- Identify your weak areas, points of failure, and potential hazards.
- Collaborate and plan with your key vendors or similar organizations in your area in order to continue your critical business operations—what you can do for yourself and what you need help with.
- Train and plan for various disaster scenarios and situations.
- Plan effective communications, which should include outside access to a variety of carriers, both wireless and local exchange.
- Identify emergency power plants throughout your campus.
- Identify security access plans and policies. Make sure these plans are available to all key personnel.
- Identify your key personnel, first responders, crisis management teams, various upper and middle management teams (Emergency Response Plan Council).
- Identify the location of your campus control room or emergency centers and equip these areas to handle all types of emergencies.

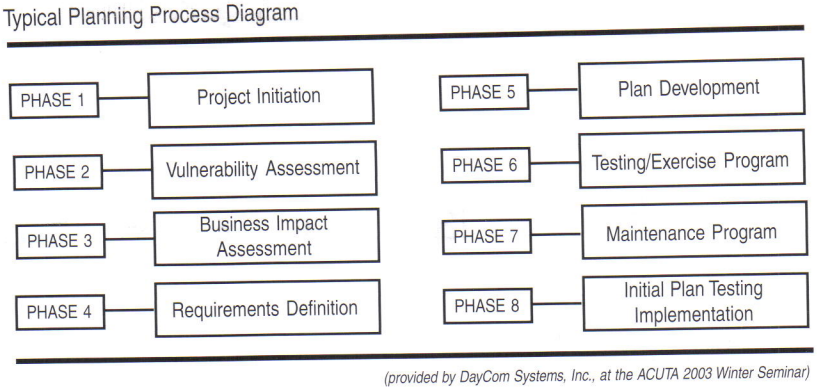
- Identify the location of recovery facilities—this could be as simple as a tent or another building location.
- Last, but not least, there should be a plan to reestablish the resources of the institution to a predisaster condition. This should include contingency funds set aside for this purpose.

As Geoff Tritsch, president of Compass Consulting, said, "A disaster plan is a major project involving both one-time and ongoing commitment of resources. Data gathering, consensus building, and writing the plan are going to take resources and require an executive champion. So you will have to sell your plan to executive management and get buy-in for political and financial support."

Include these departments (whatever your campus calls them) in your plan:

- Campus security
- Campus safety officer

Typical Planning Process Diagram



(provided by DayCom Systems, Inc., at the ACUTA 2003 Winter Seminar)

- Risk management team
- Student affairs team
- Fire safety officer
- Public relations team
- Physical plant team
- Hazardous materials response team
- Relevant community agencies

I have just touched the surface of what a good disaster plan should include. Presenting Georgetown University's experience during 9/11, Chris Peabody stated, "You have to be proactive, but things are still going to happen."

I encourage each of you to read the articles in this journal. Be proactive and take advantage of as many available redundant resources as your institution can afford; weigh the risks and plan accordingly. As John Wooden, UCLA basketball coach, said in 1948, *Failure to prepare is preparing to fail.*

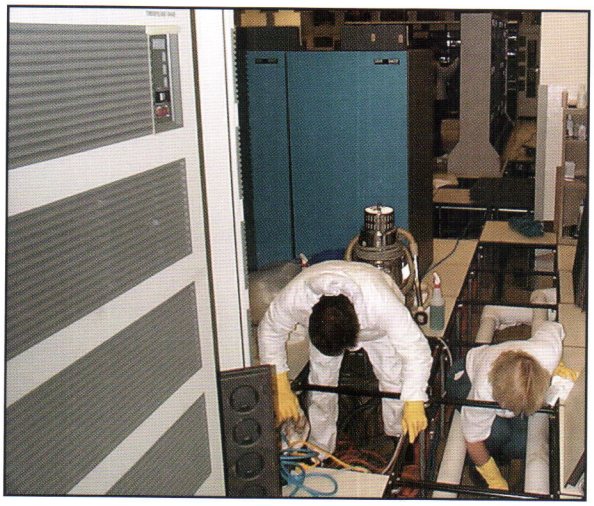
▼

Little Details Become Big Issues When Disaster Strikes

by David McDaniel

Telecommunications administrators are charged with providing and protecting voice calls, data transmission, video services, backup services, and the routers, switches, hubs, and bridges plus the cabling or wireless transmission media for all of these. They are also responsible for the portions of the facilities associated with these services. Considering an overview of disasters from a restoration perspective may help us prepare for such eventualities.

When disaster strikes, mayhem rules! After the 9/11 catastrophes, many buildings in New York City were simply demolished. The surrounding area had to deal with interrupted networks, damaged major POPs, and access problems in reaching facilities—all of this on top of the obvious emotional crisis caused by the explosions, fires, and loss of life.



Employees beginning a sub-floor cleanup in a live office. This requires great care and special equipment. The only vacuums used have electrostatic discharge suppression, HEPA filtration, and electromagnetic-interference shielding.

Blocks away, windows were blown out, structures damaged, and the building contents exposed to the ravages of the environment. Circuit boards and other internal components were blanketed with the fine dust from pulverized building materials that covered not only the surface but inside electronic equipment as well. When combined with water vapor, many of these contaminants will increase surface conductivity and cause corrosion that may degrade reliability of electronic equipment.

After tropical storm Allison blew through Houston in June 2001, many buildings were left with four to five feet of muddy water running through them. Some buildings were completely submerged. In March 2000, a major tornado devastated downtown Fort Worth. Again, windows were shattered, glass debris lined the streets, and office contents were exposed to the outside elements. It was an earthquake in March 2001, that caused similar damage to many Seattle buildings.

While the circumstances of losses change, the basic tenets of restoration and emergency response remain the same. First, preplanning simplifies response and provides a roadmap to recovery. The first response (after life, health, and safety) is to stabilize the loss site and stop additional damage. This step facilitates sound restoration/replacement decision-making; expedites the return to normal operations; and preserves critical equipment, documentation, and data.

Second (or possibly simultaneously), business continuity is accomplished, and restoration and reconstruction are begun. Sometimes, emergency response and restoration of communications depend on satellite, cellular, and radio capabilities.

Preplanning

The preplanning phase starts with a business interruption analysis to convert any interruption of services to its cost in dollars per day/hour and to define the critical departmental hierarchy in a real-cost manner. This identifies where the initial efforts are concentrated and how recovery should advance. Then the risks are delineated depending on your physical location and assets. Decisions are made based on proactively or reactively responding to these possible scenarios, a written business continuity plan is generated, and work groups are defined and trained to respond as required. Where outside expertise is called for, vendors are identified and precontracted to provide specialized services. Some of these may be structural engineers, archivists, curators, insurance personnel, health professionals, service personnel, or restoration experts.

A number of routine habits can minimize loss from disasters. Turning off workstations when they are not in use, returning magnetic media such as tapes and floppies to proper storage after use, and avoiding small electrical space heaters in offices are some small steps that can pay big dividends. Redundant fiber backbones, multiple-building cable entries, sealing cable runs in utility closets, locking closets with hubs and routers, and separating large UPSs containing lead acid cells (or network battery plant) from the electronics air supply can also prevent service interruption. Pre-wiring electrical supply lines to an external connector box and providing switch-over capability will allow rapid connection to emergency power generators for important equipment.

During this process you should familiarize yourself with the public sector disaster-response plans. Where will the emergency operations center be located? Who will be the incident commander? Work with them so they know your response needs. Where do you need access? How many people will be involved? What time frame are you dealing with? How will you identify your people so security may be maintained?

Stabilization—Stopping the Damage

In a fire, carbon monoxide and other acidic, corrosive, toxic, fire by-products are often formed. One of the most common products in an office is PolyVinylChloride plastic (PVC) which, in the presence of heat, converts 60 percent by weight to hydrogen chloride gas. When combined with water vapor this gas forms hydrochloric acid. Other products will convert to sulfates, nitrates, and even poisonous cyanates. The smoke is totally analogous to fog diffusing throughout the building. It has a dew point temperature and condenses on surfaces below this dew ▶

point. It is concentrated inside equipment with cooling fans. More monetary damage is done each year by smoke than by heat from fire. More people are overcome by smoke than burned.

Small, calibrated digital instruments are available to measure the basic chemical properties of residues at a loss site. Measurement of halogenide surface concentration, pH, and total ionic surface concentration can define the severity of smoke damage. Visual assessment of thermal damage and soot concentration will also help. This is an area in which experienced, properly equipped, disaster-restoration personnel can be invaluable.

Water inundation—whether from fire suppression or from hurricanes, tornados, tropical storms, and floods—will lead to secondary damage due to microbial growth and material decomposition in addition to the initial damage if not properly addressed. Please note that floodwater is a biohazard, carrying with it bacteria, chemicals, wastes, and viruses. Anyone exposed to this water should take all reasonable precautions such as wearing proper clothing, gloves, and boots. DPT and hepatitis inoculations are also recommended.

The most important step in stabilization of a wet building is control of moisture. Removing wet debris and drying the building environment with commercial desiccant equipment will prevent secondary damage and protect metals from the devastation of corrosion. The refrigerant HVAC system is not designed to deal with such a latent moisture load and is usually inadequate to generate rapid drying. If such control cannot be accomplished on site, contents must be moved to a protected area and structural components covered with a protective lubricant. Critical communications areas may be segmented and supplied with dehumidified air if someone monitors heat that can quickly exceed equipment-operating temperatures.

A building cannot be dried too fast, with the notable exceptions of wooden musical instruments and museum artifacts. Moisture removal dramatically slows corrosion of exposed metal. Strategically placed, small, digital battery-powered logging hydrothermometers may be used to monitor the drying process. Direct probe and capacitively coupled moisture meters may be used to determine water content in building materials and interstitial spaces to ensure complete drying.

Wet paper and archival documents should be quickly packaged, inventoried, removed, and frozen. Later they may be freeze dried and cleaned to minimize the damage and return a usable paper document. Wet recording media such as magnetic tape, optical or magneto/optical disks, microfilm, microfiche, x-ray film, and photographic media should also be packaged, inventoried, removed, and frozen. These media may be thawed at a later time for specialized wet processing to recover the data. In all cases, initial freezing stops additional damage and allows for restoration recovery.

Before packaging documents for freezing, determine the size of modules that will allow for separation during the restoration process. Freezing a box of wet documents will result in one large block of ice. Separate modules with plastic wrap, freezer paper, or wax paper. The module size may be a file folder, a file drawer, or even office-by-office. Irrelevant documents and data media may be discarded and valuable documents and data media restored during restoration.

Severely water- or heat-damaged equipment should be inventoried, moved to a storage area, and kept until disposition is decided by a representative of your insurance company. Under no circumstances should any item of significant economic value simply be discarded.

Restoration

The restoration process for electronic equipment that has not been thermally damaged involves the removal of all contaminant deposited in and on the equipment. The equipment may require complete dismantling and cleaning with high-pressure, deionized water and nonionic surfactants. It may be as simple as opening the equipment and vacuuming with a static-electricity-discharge-protected HEPA vacuum. The level of cleaning is defined by the simple chemical tests mentioned above. The same tests are used as quality control to ensure the return to original factory product-engineering specifications of cleanliness. The equipment is then tested, diagnosed, and serviced as required to recertify it for operation by the service organization contracted to the university.

Electronic restoration is scheduled around operations. Switches may be done one node at a time. The restoration is done after the network is rerouted around affected equipment and cabling to avoid service interruption. Spares are brought in on standby for critical equipment to ensure service restoration after cleaning. Laboratory equipment is recalibrated by the appropriate organization to maintain NIST traceability.

For the building, the restoration process involves cleaning all exposed

surfaces of structure and contents: cleaning the HVAC system including air returns (also dedicated Leibert units), cleaning elevator shafts, and sealing interstitial spaces as needed. Deodorizing and disinfecting may be required in some cases. In any loss where inhabited spaces have been affected by significant amounts of residues, whatever the cause, the services of a certified industrial hygienist may be enlisted as a health professional to oversee the use of chemicals and processes, and to recertify the building for reoccupancy.

Specifics—By the Numbers

The soot plate left from condensed smoke generated by a fire that has consumed plastics and elastomers (i.e., electrical cable and wire insulation) is a greasy, waxy substance composed of carbon, oxidized organics, and other by-products such as those discussed above. The presence of carbon on the surface of electronic equipment degrades the dielectric performance, especially in high-frequency and high-impedance applications.

The scale of surface concentration is bounded on one end by MIL spec 28809A that requires no more than 3.1 micrograms sodium chloride equivalent (SCE) per square cm for military electronics. This is the definition of a clean board. Some manufacturers, such as IBM, have a more stringent requirement of 2.2 micrograms SCE per square cm. On the other end of the scale, experience by Bell Core labs in Hinsdale, Illinois, has shown that any PC boards with a halogenide surface-concentration level above 62 micrograms SCE per square cm cannot be reliably restored.

The basis of MIL spec 28809A is a measurement of the conductivity of a deionized-water wash solution derived from a printed circuit board rinse. Since the deionized water has very low conductivity, the measured conductivity is primarily caused by ionic contaminants deposited on the PC board surface, and the resultant measurement is calibrated in micrograms SCE per square inch. We use the Horiba twin conductivity meter to measure the same quantity. The Saltesmo test correlates very well with this measurement when the contaminant is solely from the halogenide family. This test is more accurate than Saltesmo because it is not ion specific.

Chlorides are a part of the halogenide group. A chloride corrosion problem is compounded by the insidious nature of the chemical reactions between ferrous metals and hydrochloric acid (HCl). The HCl reacts with iron to form ferrous chloride (reaction 1 below). Ferrous chloride is not stable and reacts with water to form a ferrous hydroxide *and hydrochloric acid* (reaction 2). The hydroxide reacts with oxygen to form rust and water (reaction 3).

Reaction 1: $Fe + 2HCl \rightarrow FeCl_2 + H_2$ (gas)

Reaction 2: $FeCl_2 + 2H_2O \rightarrow Fe(OH)_2 + 2HCl$

Reaction 3: $4Fe(OH)_2 + O_2 \rightarrow 4Fe.OH + 2H_2O$

Just as in the case of salt corrosion, which is a more familiar form of corrosion, the process continues until *all the metal is corroded* because in the second equation HCl is generated and can attack more metal. The most noxious thing about the reaction is the cyclic ▶

Quotable

System failure—not terrorism or vandalism—is what is going to get you.

Steve Hailey, project engineer
Daycom Systems

Policies and procedures are not something you write once and put on a shelf. Make sure they reflect operational realities and lessons learned. They are the best way to develop consensus across business units and ensure continuity of operations over time.

Michael Zastrocky, consultant
Gartner, Inc.

Play the Achilles' Heel game with your network. Find the hidden vulnerabilities in your network. Then fix them.

Chris Peabody, director
Network & Security Systems
Georgetown University

nature of the reaction. The input is metal, the output is rust and water, and the acid is free to react again and again. The surface concentration of HCl, the temperature, and the ambient humidity determine the speed of this reaction. Halogenide surface concentration levels may be rated as follows.

Halogenide Surface Concentration

Micrograms SCE /sq. cm.	
1 – 5	Normal Background
5 – 10	Light Contamination
10 – 15	Moderate Contamination
15 – 20	Severe Contamination
S > 20	Very Severe Contamination

High surface-concentration levels of halogenides (suggested limit 11.6 micrograms SCE per square cm) in the presence of moisture cause continuing corrosion to occur on uncoated metal components.

Any moisture measurements are converted to specific humidity levels measured in grams of water per kilogram of dry air. This number is a good indicator of moisture content and does not vary with temperature. The desirable level of moisture occurring at 22°C and 50 percent relative humidity is 8.7 g/kg. Corrosion is slowed at this moisture level. Above 12 g/kg the corrosion is rapid, increasing with the level of moisture.

Initial Response

The first warning signs will be the corrosion of mild steel hardware components. *The most effective means of corrosion control is to lower the humidity to reduce the reaction rate.* Remove water. The steps are as follows:

WARNING: DO NOT ENERGIZE ANY WET EQUIPMENT—REMOVE POWER

- Open cabinet doors, remove side panels and covers, and pull out chassis drawers to allow water to run out of the equipment.
- Remove standing water with wet vacs. Use low-pressure air (50 psi) to blow trapped water out of the equipment. Absorbent cotton pads (such as diapers) can be used to blot up water. Use appropriate caution around header pins and backplane wire wrap connectors to avoid bending.
- Vacuum and mop up water under any raised computer-room floor.
- Equipment that contains open relays and transformers will require a special bake-out before application of power.

Conclusion

Knowledge is a powerful ally—especially in times of stress. Knowing the threats allows you to gather required materials ahead of time, assign personnel, and plan your path to recovery. Simple actions minimize damage, allow continued services, and expedite return to normalcy. Learn your university's business continuity plan and then tweak it for your department's specific needs.

David McDaniel is chief scientist of BMS Special Technologies Division in Fort Worth, Texas. Reach Dave at 800/433-2940.

Basics of Disaster Preparedness

by Ron Walczak

Any campus that hasn't put a great deal of thought and planning into how it would respond in a crisis is courting disaster. Certain specific actions can and should be taken to prepare an organization for recovering systems that have been damaged or destroyed by events beyond our control. At the same time, as important as our businesses and systems are, we must configure our plans around the ultimate goal of disaster planning—the protection of human life. Integrating that thread into your disaster plan will add just a few extra, but important, steps.

Definition of a Disaster or "Event"

If you are going to develop a disaster recovery plan, it makes sense to first define the events that will trigger a plan's implementation. The best plans are capable of addressing minor emergencies, full-scale disasters, and other crises in between. You will find that by gathering the information needed to address a full-scale disaster, you will have also gathered the information necessary for consistently dealing with smaller events.

Each institution should define its own events based upon internal criteria specific to the institution. Major events should include such scenarios as the following:

1. An event has disabled, or is expected to disable, the computing facilities and/or the communications network to the degree that normal operations will suffer significant impacted for a period of 24 hours or more.
2. An event beyond the scope of daily operations has impaired the use of computers, telephones, or communication facilities in a manner that will substantially affect the normal operation of the institution.
3. An accident caused by problems with computers or communications systems or equipment managed by the institution has resulted in the injury of one or more persons.

General situations that can destroy or interrupt computer and telephone services occur under the following major categories:

- Power interruptions
- Air conditioning or other environmental interruptions
- Fire
- Water
- Weather or other natural phenomenon
- Sabotage, interdiction, or network security breach.

Each of these categories warrants an appropriate response plan. When combined, these constitute a total, but modular, plan.

Disaster Recovery Team Organization and Member Responsibilities

A plan is only as good as the team that uses it. A disaster recovery team (DRT) should include the management people who have both the ability and the authority to allocate resources and funds as well as the operational personnel who will actually fix the problem presented. Conducting a successful and efficient salvage operation after a disaster requires activation of a team that should be established before any emergency occurs. The purpose of a DRT is to:

1. Ensure that all reasonable measures have been taken to prevent a disaster from occurring.
2. Ensure that employees in the respective units are advised of emergency proce-

▶

dures, locations of fire alarms and extinguishers, evacuation procedures, and locations of emergency exits.

3. Assess and assist during any emergency whether during or after business hours.
4. Direct the flow of people during an emergency to the nearest emergency exits in the quickest and most orderly fashion.
5. Direct and supervise recovery operations to salvage the maximum amount of materials in a manner that will minimize future restoration costs and effort.
6. Coordinate personnel.
7. Identify vital records and establish recovery priorities.
8. Arrange for equipment, supplies, and space.
9. Designate a person in charge of public affairs.

The DRT's collective mission is to evaluate the situation quickly, make assignments, gather needed equipment and materials, set up work areas, and remove damaged records from the affected storage areas.

If a disaster occurs in the building during nonworking hours, the director of information technology (substitute your organization's title) is designated to receive the first call, assess the problem, and initiate the phoning of others if necessary. In the event of a disaster, the DRT should be ready to meet day or night.

Disaster Recovery Team Organization

The team should include people with the following functional responsibilities (titles may vary):

- Disaster recovery coordinator
- Director of IT
- Director of telecommunications
- Director of network and security
- Director of applications and client services
- Insurance/internal audit team

Disaster Recovery Team Headquarters

Where will you gather is not an insignificant question. Depending upon the event, you may not always be fortunate enough to get close to the scene.

Preparation

It is not easy to adequately prepare for disaster events. Most of us remember fire drills from our grammar school days. They always went smoothly, the path to the doors was always open, and there was always an adult to show us where to walk (not run). The 9/11 attacks demonstrated that while conventional wisdom does not always work, it sure increases the odds in your favor! We've all sat through the airline safety announcements; like you, I usually am reading something or looking out the window to see if my luggage is going to make the flight. But one sentence gets my attention every time: "The nearest exit may be behind you." The location of the exits with reference to my seat changes every time I fly, so common sense dictates that I make note of the new information.

Documentation

You do *not* have enough accurate documentation. The sooner you admit this truth, the more time and thought you can put into filling the holes. The key to rebuilding is having accurate and current documentation on the existing systems and layout. This information must be duplicated and stored in a secure location (off-site).

1. Computer/telephone room and tape library layout (includes the physical construction, electrical requirements, and environmental requirements of the computer room and the filing system for tape backups)
2. The power and cabling diagrams for the computer/telephone room (this includes all communications cabling between devices)
3. The air conditioning, fire suppression, and keypad lock system documentation
4. Computer equipment and vendor by location and serial number (helps with insurance claims)
5. Software systems and data-entry procedures
6. Configuration information
7. Line flow-chart drawings
8. Contacts
   - Employees
   - Utilities (telephone, electric/gas)
   - Equipment/software suppliers
   - Office equipment/supplies
   - Emergency support for hardware and software
   - Reclamation company
   - Moving company

Security

Think for a moment about the potential security issues that arise when a disaster strikes. Security concerns must go beyond worrying about things like equipment disappearing (which can happen). What about paper and electronic records that might become accessible through the process of throwing away damaged equipment or files? You must develop procedures to address the following:

1. Building access
2. Authority to make "discard/retain" decisions about damaged media
3. Secure disposal of sensitive material and equipment

General Issues

Activities and responsibilities for each of the following actions must be performed on an ongoing basis to ensure IT's readiness for any potential service interruption:

1. Maintain and update the disaster recovery plan.
2. Ensure that all IT personnel are aware of their responsibilities in the event of a disaster. Don't forget that new employees must be trained!

3. Ensure that the periodic rotation of backup media to off-site locations is being followed.
4. Maintain and periodically update disaster recovery materials, specifically documentation and systems information stored in off-site locations.
5. Ensure that operations procedure manuals are kept current with copies stored off-site.
6. Maintain current status of equipment and circuits located in the equipment room.
7. Prioritize all systems for recovery.
8. Assign responsibility for all applications.
9. Designate systems requiring detailed recovery plans.
10. Ensure that emergency lighting and power systems are properly functioning and are being regularly tested by facilities and operations personnel.
11. Ensure that fire- and smoke-detection systems are being routinely tested and are functioning properly.
12. Ensure that proper environmental standards are being met in equipment areas.
13. Ensure that the client community is aware of the concept of disaster recovery, of procedures you have enacted, and of how a disaster could affect normal operations.
14. Ensure that all personnel are aware of proper emergency and evacuation procedures.

Testing

So, now that it's documented and organized, how do you test? First, realize that your organization probably does not place as high a value on your systems as you do. Not only is it inconvenient, it also takes time and money to test disaster recovery plans, and it is unlikely that you want to simulate total disaster conditions! Realistically, you can schedule tests for recovering individual systems to determine how long it takes and what pieces are missing from the plan. I alluded to a modular plan earlier. The more individual systems you test, the more confidence you will gain in being able to handle them consecutively if necessary.

Conclusion

I hate paying for insurance. Every time I write a check to pay a premium, I see insurance as a cost—one I do *not* want to have to recover. Planning for recovering systems is like that. We are all so busy, and taking systems down to test recovery plans is probably not high on most people's lists of things they want to do today. On the other hand, I have collected against insurance policies; I have also recovered days and weeks of effort because my systems were properly backed up. It's during those moments that I realize the time, effort, and cost of preparedness was an investment, not a cost. Take the time; plan the plan; and then, if you have to, work the plan when trouble hits. You'll thank yourself later for being so forward thinking!

Ron Walczak is the principal consultant with Walczak Technology Consultants, Inc., in Prospect, Pennsylvania. Visit his Web site at www.walczakconsultants.com.

Power Backup Assures Network Continuity: Motherly Advice on UPS

by Curt Harler
Contributing Editor

(Note: This article contains information that is product- and company-specific. ACUTA does not endorse products or companies, and references provided in this article are intended for information only. As always, we recommend that you make decisions based on your own evaluation of a vendor's products and services.)

Your mother could have been a great network manager. She had the right idea about assuring things went well. She would have handled a telecom or computer network just like she did your ears. Keep your ears clean and keep them open, she would advise.

Instead of applying soap and water, port Mom's advice to the telecom closet. What works best to keep things running is a properly engineered uninterruptible power supply (UPS) system. A well-designed UPS not only assures continued power in the event of an outage but also evens out the spikes and dips in power.

For those starting out, a good rule of thumb is to try to provide as much power backup as possible in a single package. Some are reluctant to put all of their eggs in one basket—but it is much easier to keep your eye on one basket than on scattered ones. From a practical point of view, a single, large system is easier to maintain and to service.

Another thing to keep in mind, especially when protecting telephone lines, is that the tip and ring may or may not be grounded. Digital subscriber lines (DSL), especially, tend not to be grounded. Digital lines have three places where there can be a potential difference: between tip and ring, between ground and tip, and between ground and ring.

Companies like Leviton Manufacturing (www.leviton.com/powerquality, Little Neck, N.Y.) offer 19-inch rack-mounted surge protectors. Their latest line offers point-of-use transient-voltage surge suppression for rack-mounted equipment. Each has 12 protected receptacles, 10 in back and two on the front. Models are available with either 15- or 20-amp receptacle ratings and a choice of straight-blade or locking plug. We'll talk about specific products later.

According to an Electric Power Research Institute (EPRI) study, the average plant in the United States experiences 66 power sags a year. The cost per incident ranges from $6 to $40 per kVA per event. EPRI puts the cost for a 500 kVA system as high as $20,000 per event; at 66 sags a year, that's a potential cost of $1.32 million annually.

Standards: Setting the Rules

Just as Mom had rules for most occasions (and was willing to make up new ones as she went along), there are several basic guidelines to follow when specifying a UPS or assuring clean power to the network.

Standards are a good place to start with telecom, computer, or other electricity-reliant systems. Two basic standards come into play when protecting these systems. The first is UL-1459, which addresses power concerns from the end user's point of view. The second is the FCC's Part 68, which deals with protecting the telephone network. Both of those specifications have been around for a

long, long time. A telecom manager should, at least, be familiar with them.

Early on, gas tubes were used to protect systems against surges and the like. Later, metal oxide varistors (MOVs) took the forefront. MOVs are basically voltage-dependent resistors. They absorb voltage and current surges or spikes using a solid-state thyristor approach. Some products such as the SIDACtor from Teccor Electronics (www.teccor.com, Irving, Tex.) make use of voltage breakdown on the thyristor, giving highly controlled, consistent protection. Units are available from 30 to 400 volts, with 300 being typical for protecting phone circuits. Telephone lines typically are -48 volts DC, but the ring voltage will be clipped with a unit like a 60-volt protection system.

The thyristor switches in less than a nanosecond, making it predictable with minimal overshoot. When the trigger voltage is exceeded, energy is dissipated in the copper wires. The unit resets itself when the current goes away.

Such units are available in sizes as small as 500 VA to sizes rated in the multi-megawatts. Invensys (www.invensys.com, London, England) offers IT managers a complete line of double-conversion UPSs in its Axxium Pro line. The system can be provided with more than one backup unit and can be daisy-chained by adding additional modules.

A double-conversion UPS is perhaps the most reliable solution for isolating input transients, regulating the output frequency, and providing the purest output 100 percent of the time.

Especially in areas like California where extended blackouts are common, it is important to provide fuel for extended use of the generator. The more efficient the UPS, the longer the generation time. The engine can be smaller or run longer.

Inspections: Let's Get Physical

Mothering is just as important with power systems as it is with kids. Not only should there be a schedule to check the obvious, like diesel fuel levels in emergency generators, but physical connectivity should also be inspected regularly. It seems redundant to emphasize that all wiring has to be tightened down, but that is a common cause of failure, according to Henry Lengefeld, senior staff engineer with American Power Conversion's (www.apcc.com, West Kingston, R.I.) enterprise systems group.

"It's one of those tests you have to do annually," Lengefeld says. "In a critical data center it should not be put off." One way to avoid having to take the system offline is to use an infrared camera to check for hot spots and then decide how urgent the situation is.

Lengefeld recommends checking compatibility of the engine-generator with the UPS. "The contractor must be sure it is sized to the UPS," he says. The closer it is to a 1.0 power factor, the better. Contractors should look for a UPS with low input harmonics, as well.

Hook up customers to a system that gives a "soft start" so the power can come up in a controlled fashion.

Look at Offerings

This past fall several firms, including APC, GE Digital Energy (www.gedigitalenergy.com, Atlanta, Ga.), Clary (www.clary.com, Monrovia, Calif.), Leviton, Main Power (www.mainpower.com.tw, Taiwan), MinuteMan (www.minutemanups.com, Carrollton, Tex.) and Tripp Lite (www.tripplite.com, Chicago, Ill.) brought out new lines of UPSs. We'll look at them in order.

- **APC** expanded its Smart-UPS line with a new one-unit rack-mount UPS, available in 750 VA and 1000 VA. It offers both USB and serial connectivity. A built-in expansion slot integrates with the product's power management accessories. This allows network managers to monitor their UPS via standards-based systems such as the Web, SNMP, WAP, telnet, DHCP, or Syslog.

In addition to taking up less rack space, the new units provide a wider input voltage range that can maintain computer-grade power without the UPS utilizing battery power even if nominal voltage drops by 30 percent.

- **Clary** offers a new 19-inch, rack-mount, direct-conversion unit. "This gives true, clean, regulated power at all times," according to Joseph Palsa, director of sales. Even at 85 volts, it maintains nominal 120 power.

Clary claims to have the most reliable product on the market. It has many good, specialty products in the UPS area that are of interest to colleges. For example, schools with hospitals would be interested in Clary's FDA-listed 1250 VA UPS for ventilator use. Clary even has a special model aimed specifically at supporting the traffic signals found on many urban campuses. ▶

In addition, the company markets products aimed at supporting the E-911 arena. Palsa notes that all of the E-911 in Massachusetts is backed up by Clary's product.

- **GE's** Signature 5000 Series is targeted at improving performance and reliability for mission-critical applications. This three-phase UPS system provides critical power protection for a wide range of applications, including telecommunication operations, healthcare, and information technology systems. The producer, GE Digital Energy, a unit of GE Industrial Systems and the General Electric Company.

The first phase of the North American Signature launch will be for products ranging from 10 kVA to 150 kVA. Additional products within the Signature Series will be introduced globally in 2003.

The Signature 5000 Series operates in a double-conversion mode, with true online voltage- and frequency-independent operation, resulting in maximum levels of power reliability. In addition, the Signature 5000 systems can be paralleled by up to eight units using GE's unique Redundant Parallel Architecture (RPA), ultimately achieving redundancy or increased power capacity in a flexible and cost-effective manner.

The Signature 5000 Series is built for extremely low output voltage distortion, reducing the need for over-sizing the UPS. It also offers space vector modulation, resulting in faster response and higher efficiency; an output isolation transformer to separate the utility power from the load, providing greater critical power protection; and superior battery management, enhancing the life of the battery and reducing operational costs.

New features of the Signature 5000 Series include front service access that reduces operational footprint, maintenance, and repair costs; enhanced cooling design, increasing reliability and availability; integrated input filter, reducing the input current distortion; and an automatic start-up procedure with a user-friendly interface.

- **Leviton's** existing Lev-UPS line was enhanced with its On-Line and Pro models. Both are focused on mission-critical data processing, telecommunications, and security applications.

The double-conversion design provides the highest level of power protection. Connected equipment is immune to slight power fluctuations and is protected from spikes, surges, noise, extended under- and over-voltages, harmonics, and frequency variations.

All On-Line models feature a wide input voltage tolerance and output with less than 3 percent total harmonic distortion. Twin microprocessors aid redundancy, and an automatic bypass switch ensures that power to the load is not interrupted in the event of a UPS fault.

The Lev-UPS Pros provide up-to-the-minute sine-wave tracking and control firmware to improve response time and efficiency. All models have line-interactive, tap-changing Lev-CON technology to mitigate sags and swells without relying on backup battery power. This conserves the battery for more severe disturbances like power interruptions or outages. Units are available in 2-KVA and 3-KVA versions in either tower or 19-inch rack-mount configurations. Both line-interactive and online topologies are available. All offer power monitoring and UPS control software, along with 120-VAC nominal input (as opposed to the previous 115-VAC rating).

- **MinuteMan's** SmartSine Series is designed for networking and communications systems. Each unit provides line-interactive design with a true sine-wave output. It uses the company's independent battery bypass technology, which allows the UPS to continue to correct and condition incoming AC power without shutting down output power, even if the UPS batteries become discharged or disconnected.

At their support Web site, www.sizemyups.com, MinuteMan offers a handy, automated guide to assist telecom and network managers in configuring the system load used by equipment and calculates the UPS requirements (given in terms of MinuteMan's product line, of course) for the system.

- **Main Power** has a smart online rack-mounted UPS that uses double-conversion technology to ensure fully regenerated sine-wave output independently of the utility's supply.

The CE- and UL-listed units are manageable over RS232 and SNMP network controllers and offer self-diagnosis for any operational problems. They are two rack units high. The inverter in the UPS continuously pulls power from a completely independent DC source, thus protecting the connected load from power-related problems.

Quotable

Universities are open institutions. Few were ever thought of as targets until the Unabomber. But just stop and see the university through the unfortunate eyes of one who sees you as the center of all evil. These people exist and sometimes are employed by you. Your responsibility is to take preparatory measures to mitigate what they could possibly do to your students, staff, and communications. If you do not believe these things in your heart, you are a misfit at this job in this era of terrorism.

Robert A. O'Neil
O&A Engineering

Some security directives for WLANs:

- Change the security. Do not use default SSID numbers or null SSIDs.
- Use 128 DES with dynamic session keys. Do not use 40-bit WEP.
- Implement message authentication code (MAC) address tracking to control network security.
- Monitor access logs: Track network access attempts via IP addresses. If an attacker attempts access, the logs will point to the source address and make it easier to track and stop.
- Evaluate physical security perimeters. Where possible, observe the grounds to the limits of coverage and advise the security department to look out for suspicious activity.

Michael Zastrocky, Consultant
Gartner, Inc.

Set expectations before others set them for you. McDonald's restaurants solve problems for hungry customers in 30 seconds. Customers don't know or care about what goes on inside the kitchen. All people know is their problem—they are hungry—is solved in 30 seconds at the drive-through window. People today expect instant gratification. If you don't set reasonable expectations, people will set unreasonable ones for you.

Charlie Moran, Vice President
Blackwell Consulting

• **Tripp Lite** has true, online UPS in ranges from 1000–6000 VA. Their dual-conversion technology continually converts incoming AC power into filtered DC power and then resynthesizes it back into AC power with a pure sine wave. One handy feature is the ability to prioritize the uptime of the most mission-critical loads during a power failure. These models feature special receptacles that are controlled independently, letting a manager shut down less important systems, preserving battery runtime for the critical applications. The units are designed to adapt to towers, on base stands where space permits, and to rack-mount uses, with removable rack hardware.

Upgrading

Rather than planning to replace an existing UPS with a larger unit to handle any increased load, look into starting out with a scalable UPS. They can be paralleled together, increasing capacity.

A secondary benefit of scalable UPS is the redundant protection provided for mission-critical applications. By paralleling several units together, one of the units can serve as a backup to any of the others in the event of a UPS system failure.

Mom would have told you that you came with two ears (and one mouth) so you could listen twice as much as you talk and so you could keep out of trouble. Oh, and that ringing in your ears? It has nothing to do with telephony. You'll have to ask your mom about that.

Curt Harler is a contributing editor for the *ACUTA Journal* and a freelance writer who specializes in communications technology subjects. Contact Curt at curtharler@adelphia.net.

Preparedness, Continuity, and Restoration of Telecommunications

by Charles V. Bryson

In the early 1970s, I was walking a patrol beat on the midnight shift as a campus police officer at Virginia Commonwealth University when I heard the distinct sound of a water-flow alarm coming from an area near the president's house. As I turned the corner, I could see flames erupting from the president's office. Just that evening, I had been issued a brand new, state-of-the-art, two-way radio, which I quickly grabbed to call for help.

"114 EMERGENCY; 910 West Franklin, 10-70 structure!" I exclaimed into the radio. Strangely, there was no reply to an emergency call, which had priority over all other radio traffic. Once again I called into the radio, "Unit 114 EMERGENCY, I have a signal 10-70 at 910 West Franklin." This time the dispatcher replied, "Unit calling radio, you are unreadable."

Though I'm sure Ozzy Osbourne would have recognized them, time has kindly erased all the expletives that I surely used that night, as I ran across the street to an emergency telephone "call-box." I pushed the special police button and quickly got a dispatcher who notified the fire department to respond to what became a two-alarm fire started by an arsonist. At that time in my life I came to appreciate the value of a redundant communications system. Thirty-plus years later, the importance of redundant systems has not diminished.

Campus administrators recognize that the institution must often provide the same public-safety services as a local government. The heart of a campus public-safety department is typically the communications center. In the post–September 11 world, reliable voice, data, and wireless communications systems are absolutely essential, and campus public-safety offices must be provided with secure and highly redundant telecommunications services. A campus public-safety office operating a communications center at a lesser standard invites many operational problems and threats to the welfare of faculty, staff, and students, not to mention potential litigation. Although all of us would like to believe that the campus is a safe haven for students and faculty, the reality is that the targets of today's terrorism are only limited by the imagination of the terrorist.

Disaster Management

Disaster management addresses preparedness and prevention, operational continuity during a disaster, and service restoration following a disaster. Although many people use the term *disaster planning* to mean something

more, disaster planning is only one part of the larger process. *Disaster management* is a better choice of terms because it is through important management strategies that disrupted telecommunications systems may be restored.

Preparedness

Elements of commonality often exist in campus public-safety communications systems. Perhaps the most critical systems provide voice communications into the public switched telephone network (PSTN) and control of two-way radio systems. These communications systems must be *target hardened* or protected from the campus to the local exchange carrier (LEC). As consultants, we are often amazed by the lack of redundancy from a client's site to the LEC. Even some large municipal public-safety answering points (PSAPs) are only a backhoe cut away from disaster. At one client site, a backhoe actually didcut strands of fiber coming onto a campus at the beginning of a semester, creating telecommunications disruption for two very significant days.

The first step of prevention begins with the telecommunications administrator working proactively with the campus public-safety staff to recognize their unique requirements. As an example, 911 calls may be required to go first to a central PSAP[1] off campus that routes emergency calls to the campus public-safety center or appropriate jurisdiction[2] for action. In this example, the campus public-safety office should have multiple methods of contact with a PSAP. Typically, direct-access or *ring-down* circuits are utilized to hand off an emergency call from a PSAP to the responding agency. A direct circuit, as well as traditional telephone dialing, provides multiple means of access provided that LEC circuits and central offices remain in service.

To strengthen LEC services, a typical strategy utilized by many jurisdictions is to subscribe to a synchronous optical transmission system, or SONET, coupled with independent circuits transporting telecommunications services into separate building entrance points. This strategy, when appropriately engineered, minimizes the likelihood that contact between the user and LEC will be disrupted.

Of additional importance, this same LEC transport strategy may be used to provide connectivity between the campus and PSTN as well as public-safety communications centers and *tone-control*[3] radio transmitters. Access to radio transmitter systems must be prioritized for two essential reasons. First, it is through these systems that campus public-safety resources are continually directed. Second, radio systems may be used for intergovernmental communications.

As an example, the Commonwealth of Virginia established the Statewide Intergovernmental Radio System (SIRS)that has been installed in most local governments including campus public-safety communications centers as well as state law-enforcement vehicles. Although SIRS is typically used as a strategy to permit time-sensitive intergovernmental communications, such as a campus public-safety office calling a state police car in an emergency, communications centers can communicate directly when necessary.

New Technologies

It is likely that wireless communications networks will play an increasing role in the delivery of public-safety telecommunications systems. In the proposed 2003 federal budget, President George W. Bush requested $3.5 billion for new communications equipment and training for local *first responders.* Additional money is included in the proposed appropriation for the Federal Emergency Management Agency (FEMA), and at the time of this article, Congress had not completed action on the budget for homeland security.

FEMA also will provide grants for state and local agencies to build geographic information systems (GISs), including interactive maps showing public escape routes and locations of response teams. New York has developed one of the most advanced systems. Residents can access the program on the Web and use it to get current information about natural disasters, such as hurricanes. City officials have said the system could be used during terrorist attacks to direct people to evacuation routes and to provide officials with the locations of first responders.

This new GIS application is another example of the power of the Web in addressing evolving problems. In fact, it was the GIS and skills provided by higher education that assisted rescuers at the World Trade Center disaster site. Telecommunications network services supporting both GIS applications and Web servers must ▶

Telecommunications Systems Commonly Found in Public-Safety Communications Centers

Voice Connectivity to PSAP
Voice Connectivity to PSTN
Radio Transmitter Control Circuits
Data Circuits for NCIC/State Law Enforcement/DMV
Fire/Intrusion Alarm Circuits
Emergency Call Boxes

be considered as tools in support of disaster management.

Some campus communication centers also incorporate the use of cellular telephones as a redundant telecommunications strategy. The weakness of this strategy is the traffic management capabilities of the local cellular provider. If a cellular strategy is contemplated, a cell phone should be able to reach multiple cell sites of the carrier. However, as was experienced in the northeast on September 11, when cellular networks were clogged with callers, these systems became virtually useless. Contrary to popular belief, the cellular companies do not prioritize cellular telephone access on their digital networks for public safety. There is some discussion in the cellular community relative to the prioritization of cellular telephones for public safety; however, implementation of such a system, even if permitted by the FCC and the Telecommunications Act of 1996, is uncertain.

Other campus telecommunications systems should be considered for target hardening. Many campuses rely on emergency call boxes for communications. Occasionally, these systems operate outside the campus PBX system. There is some wisdom in the use of call boxes on a system independent of the PBX. Should the PBX become disabled, these call boxes may become primary means for persons around the campus to contact public safety. This is particularly true as more and more institutions discontinue the use of pay telephones due to low use. However, for those campuses that have not discontinued the use of pay telephones, these devices, when operated independently of the campus PBX, can be incorporated into an institution's disaster-management plan.

Environmental Considerations

The design of a campus public-safety communications system is always a critical issue. Some entities design facilities without regard to the environmental hazards associated with everyday life. For example, one city constructed a public-safety center with an air-intake system that drew vehicle exhaust into the building. Another maintained a center that offered no security for the emergency power system or its fuel source. To ensure the proper operation of equipment as well as the health and safety of the center's staff, designers must be sensitive to air handling, emergency power, and access security for staff and hardware, as well as myriad other issues affecting the operation of the facility.

Why are these environmental factors important to the telecommunications department? From a pragmatic perspective, it may be your staff working in the public-safety center to restore service during an emergency. More importantly, it is the campus telecommunications administrator's responsibility to report and remedy any issues affecting telecommunications systems. In consideration of one's corporate responsibility, the telecommunications administrator proactively takes steps to ensure the operation of critical systems outside the span of his or her administrative control.

As an example, the telecom administrator may be installing a new PBX with a remote unit installed in the public-safety center. If the location of the proposed remote unit suffers from poor HVAC, that affects the reliability of equipment, most telecom administrators would be quick to point out the problem and seek remedies. The facility causing the difficulty may be completely outside of the administrator's chain of command; however, because the problem affects the operation of an important campus system, the telecom manager exercises corporate responsibility and advocates the need for repairs. In short, an administrator cannot merely ignore a problem or vulnerability just because the matter is outside of his or her chain of command. Managers have a responsibility to the institution to proactively address problems.

Continuity of Operation

In a disaster, all or some subset of telecommunications systems may be lost. In the development of so-called *disaster plans,* staffs always fail to contemplate every contingency. The reality is that even with the best planning in the world, one cannot foresee every potential disaster.

Accordingly, in this phase of disaster management, systems must be restored on a temporary basis permitting the delivery of essential telecommunications services. Basic telecommunications must be restored providing contact with the outside world and critical service systems. The

hope is that redundant campus telecommunications infrastructure and support systems will function appropriately, permitting continued operations. However, if the scope of the disaster disables these systems, essential public-safety telecommunications services must be restored.

This suggests that instead of narrow operating guidelines, staffs must be empowered with broad knowledge about resources and systems, including campus and LEC telecommunications systems and support hardware. Empowerment means that telecommunications staffs must often do something that does not come naturally to many of us—share knowledge and, in essence, teach people how to bypass the established bureaucracy.

Public-safety staffs should be empowered with operational knowledge that describes a variety of ways in which to contact on- and off-campus telecommunications resources. Such empowerment may be as simple as providing a comprehensive listing of telecommunications staff and support hardware resources for the campus, as well as its telecom services provider(s). The listing would include names, skill sets, telephone numbers, and home addresses. This permits the public-safety department to dispatch a car to someone's home, if necessary, and secure the services of an expert to restore systems. Through empowerment and in the absence of a campus telecommunications staff member, the communications center has a starting point from which to contact representatives of the LEC.

Typically, public-safety communications center staffs are entrusted with sensitive information. Because these staff members often have access to the FBI's National Crime Information Center (NCIC) and other federal and state law-enforcement information systems, employees generally receive a fair amount of screening prior to employment. In short, telecom administrators should feel comfortable entrusting campus public-safety staffs with detailed information relative to design and resources.

It is important for the public-safety communications center to have a broad base of operational knowledge and to know how to bypass the bureaucracy when appropriate. For example, one state government set up a telephone repair procedure that absolutely prohibited any user, including public safety, from contacting the LEC in the event of a problem. Instead, the user was required to report problems to the state's help desk. Perhaps this constituted a fine administrative system, but public-safety agencies were unable to initiate telecommunications service repairs when the state's help desk was out of service.

Disaster management eschews such situations and recognizes that appropriate staff must be empowered to take extraordinary actions in the event of an emergency. In the help desk example above, a public-safety center would normally follow the standard ▶

protocol; however, staff members must know how to reach someone of importance with the LEC or other relevant entity in the event of an emergency system outage. A strategy of empowerment enables people to take extraordinary actions when appropriate.

Why is it necessary to educate and empower staffs broadly when planning can define strategies in response to an emergency? As stated earlier, it is impossible to plan for every possible disaster. Perhaps the best-planned event of the 20th century was the Allied invasion of France on June 6, 1944. Thousands of persons participated in countless hours of planning designed to address myriad contingencies. As the first soldiers hit Omaha Beach that morning, most of the preplanning failed and was virtually useless. The survivors of that morning were required to formulate their own service restoration strategies under withering German machine-gun fire. These soldiers not only survived but also conquered; the typical American had been taught to do whatever necessary to survive.

Today, we would say that these brave soldiers were empowered to change the rules as necessary. Conversely, neither German commanders nor soldiers were empowered to proactively take action; and as a result, the Allied armies were successful in an invasion that could have been a complete disaster.

This example perhaps best defines the *continuity of operation* phase of disaster management. Planning is essentially a tactical exercise; and because of the wide variety of potential disasters, it is impossible to devise tactics for every potential event. However, infrastructure resources are strategic and permit users to devise tactics in response to unanticipated disasters. Strategic resources include the documentation of systems and operations, resource guides for technicians, emergency access to spare and replacement parts, and more.

While one cannot plan for every contingency, with respect to certain potential catastrophes it is prudent to have defined plans for likely disaster scenarios. For example, Florida campuses ought to plan for hurricanes; California campuses need to know what to do in the event of an earthquake. Through prior experiences, it is likely that disaster plans have emerged to cope with a natural phenomenon.

Similarly, many campuses may be especially vulnerable to fires or flooding. Disaster management contemplates tactical planning for catastrophes and requires that steps to prevent or minimize the disruption of systems be in place prior to the disaster. It also mandates defined plans for coping with disaster's effects.

Restoration of Services

Restoration becomes a function of management and begins with an analysis of the event's scope. This becomes a collaborative process and may involve public-safety staff, telecommunications, purchasing, service providers, and others. Because many institutions have defined purchasing procedures, it is always helpful to have contingency contracts already negotiated to facilitate the purchase of replacement parts and services.

It is very helpful to have pre-negotiated contracts for on-call telecommunications personnel services even if the telecom operation is fully staffed. Following a catastrophic event, many staffing resources are needed, and it is highly unlikely that the existing telecom staff can address the emergency while providing routine services for unaffected customers of the unit. Campuses that do not prepare for disasters by bidding on-call services may be charged premium rates if additional staffing resources are hired noncompetitively to cope with an emergency.

Senior relationships with industry are also helpful following catastrophic events. It is very likely that an institution's senior leadership knows top managers of the LEC and major equipment providers. Every president of a company wants brownie points with a high-visibility customer. If support from a LEC or supplier is marginal, the telecom administrator should not be hesitant to involve the senior level of the administration in seeking greater assistance and cooperation.

In addition to understanding the systems in need of restoration, management must determine what tactical or strategic planning worked and what failed. Depending upon the scope of the disaster, restoration may be as simple as some rewiring and new equipment installation or it may necessitate the construction of an entirely new facility.

Some restoration lessons learned after September 11 are important to remember. For example, it is advantageous to have supply contracts in place to provide quick turnaround of replacement hardware. However, the transportation portion of the supply chain must now be considered as all air traffic was shut down for several days following the tragedy. In the consideration of critical systems, a campus may be wise to have a supplier that can transport hardware via air *or* truck on an expedited basis. This suggests that critical suppliers must be reasonably close to a manufacturer's location.

Earlier in the article, environmental issues were briefly discussed. If a new facility must be constructed following a disaster, designers must carefully address these environmental issues along with staffing, hardware, and security issues. Planning relative to facilities should be expanded to include not only redundant power systems such as a generator, for example, but also redundant power sources for the generator, such as installed in-ground natural gas as well as available bottled natural gas or multi-fuel systems.

Conclusion

The diverse nature of disasters makes it impossible to catalogue every issue associated with disaster management. However, the essential strategies for disaster management are straightforward and easy to comprehend. First, take reasonable steps to prevent the possibility of a disaster. If prevention fails, have strategic resources available to the staff and empower those on duty to take appropriate actions to restore essential services. Finally, the restoration of systems should be a collaborative process involving public safety, carriers, manufacturers, and a host of other persons. Through mutual cooperation and strategic resources, systems should be not only restored, but also strengthened.

Charles V. Bryson is a senior consultant for RCC Consultants, Inc., and was formerly director of business services for Virginia Commonwealth University. He can be reached at 804/422-8460 or through e-mail at cbryson@rcc.com.

[1] Due to liability concerns and legislative requirements, some institutions first route 911 calls made on the campus PBX or Centrex to a regional PSAP, which in return sends the call back to the campus public-safety communications center for action. This is a very sensitive legal issue and the advice of the campus general counsel should be obtained relative to the manner in which a PBX or Centrex manages 911 calls. Centrex may also be known as Plexar, CentraNet, or Essx depending upon the LEC serving a campus.

[2] Some campus public-safety departments do not employ persons with law-enforcement authority, necessitating the intervention of the local police.

[3] If a campus public-safety system requires DC control for radio transmitters, copper circuits must be provided throughout the route from the radio console to transmitter precluding the use of SONET. Most modern radio systems employ tone control, although older systems may still utilize DC control.

Interview

Patricia Cormier, EdD

President, Longwood College

Patricia P. Cormier has served as president of Longwood University since 1996. Under her leadership, the institution has reaffirmed its time-honored commitment to preparing citizen leaders to serve the common good, while at the same time positioning itself as a high-tech, learning-centered environment that is second to none in the Commonwealth of Virginia. Known for her personal warmth, enthusiasm, and strong commitment to learning, Dr. Cormier has been a vital force in workforce preparation and economic development in Southside Virginia and throughout the state. She has been actively involved in higher education for many years, serving in leadership positions on the American Council on Education Fellows Board, the American Association of Higher Education, the American Association of State Colleges & Universities, the Southern Association of College & Schools, and the National Collegiate Athletic Association.

Dr. Cormier has master's and doctoral degrees in education from the University of Virginia and a bachelor's degree in health education from Boston University.

James S. Cross, PhD, is the vice provost of Information Technology at Michigan Technological University. A past president of ACUTA, Dr. Cross is currently serving as the chair of ACUTA's Publications Committee.

Jim Cross: Briefly profile Longwood for our readership. Describe the disastrous fire that occurred including such things as its probable cause, extent of damage to campus buildings, and significant events leading up to and following the tragedy.

Patricia Cormier: Longwood is one of the 15 public institutions in the Commonwealth of Virginia. We are a public institution, and we are the 5th most selective institution in the state. We have 4,200 students, and nearly 90 percent of those students are full-time, and almost that number live on or around the campus. That means we are a highly residential institution.

Let me give you some more background. Longwood began in 1839 as a women's institution; that was fairly typical of the South after the Civil War. Many male teachers died, and so women were brought into the field to teach, and Longwood was part of that. We were one of the institutions that used to be a feeder into the University of Virginia; but when the University of Virginia finally admitted women in 1970, many of these feeder institutions, such as James Madison, Radford, Mary Washington, and Longwood, became coeducational as well, and we've been coeducational since 1976.

We have three colleges: a College of Arts and Sciences, a College of Business and Economics, and a College of Education and Human Services. We are nationally accredited in every program for which accreditation is granted. We have a very significant position within the state in terms of the number of Virginians we serve. And, for the 5th year in a row, we have been ranked by U.S. News & World Report as one of the top 10 public comprehensive universities in the South.

The fire: The good news is that I did check with higher beings, God included, and asked how many of these do you get per presidency, and the answer was "one" if it's really big. So this was mine.

The fire began on April 24, 2001, at about 8:30 in the evening. After an extensive investigation, the Virginia State Police did not determine an exact cause, and the fire has been ruled "accidental." The fire involved four major academic buildings, three of which were our signature buildings for the campus, the oldest buildings on campus. The buildings, which were constructed in the 1890s, were under renovation at the time when the fire broke out. It was a rainy night, the wind was blowing, and the blaze grew like wildfire. Those

buildings were interconnected by roofs, so the fire traveled rapidly and extensively as it found its way into this old wood.

The fire was absolutely enormous and consumed 200,000 square feet. We had 175 firefighters, 13 fire companies, and we literally drained the water supply of the town. We used 2.2 million gallons of water from roughly 8:30 in the evening until about 5:00 the next morning, and still the fire wasn't out completely. There were residence halls that were adjacent to those buildings, and of course, our first thought was the students. I can tell you that the 350 students who were in the adjacent residence halls were evacuated within eight minutes. There was no loss of life, there was not one injury—not even a sprained ankle. And it's because, I believe, the staff understood and took very seriously the safety and security of our students.

It was a pretty horrendous situation. There were three buildings that were under renovation so faculty were not in them and their belongings were not there; but one building did have faculty offices. Thirty faculty lost nearly everything they owned in those buildings: their diplomas, their pictures, their books, their files. It was such a devastating fire, and there was so much smoke and water damage that we were not able to salvage a great deal of what was in those faculty offices. Our entire math department practically lost everything but their hard drives. We were able to save the hard drives.

Cross: What happened after the fire? What were the consequences of that?

Cormier: I knew that we were going to have to do some things right away. When I realized we were going to lose those buildings, by 10:00 that night, I had called every member of our Board, the Governor, and the Secretary of Education for the Commonwealth of Virginia. I then began to plan what we were going to do the next morning.

At 8:00 the next morning—we didn't get home until 5:00 and came back at 8:00—I met with my entire executive management team and my deans, and we assessed the situation. What had happened was that the 2.2 million gallons of water had gone into the steam tunnels underground, which meant that we had no toilets and no showers anywhere on campus. In addition, we had 30 faculty who were teaching four courses each who had lost everything—grades, exams, and papers—that had been in their offices. So we knew we had to decide whether or not we were going to continue classes or close school early.

The one positive thing was that the fire occurred two days before the end of the grading period, so we were able to close out those classes and not do final exams except for those students who felt that they could improve their grades and who wanted to take finals (I can assure you that our students were not unhappy about not having to do finals). But we needed to make that decision right away.

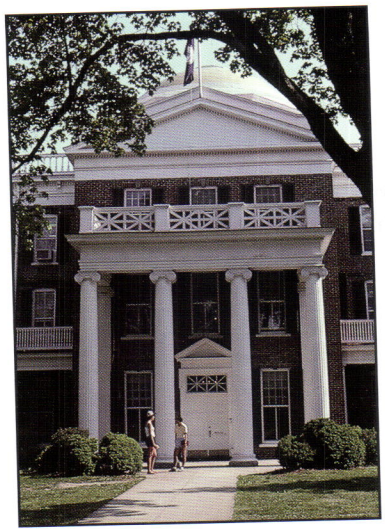
We also had to find lodging for all 350 students, so we were getting ready to set up things in our gymnasium, and as it turned out, every one of those 350 students was taken in by other students. So we didn't even have to do that. But I needed to get those students home. They could not go back into their rooms because, even though those residence halls had not been destroyed by fire, they were partially damaged by fire, lots of smoke, and massive amounts of water—not a healthy environment. It was an absolute mess. Ceilings had collapsed, and there was stuff all over the place. You know, students are not terrific about hanging up their clothes, so we had pools of water and clothes floating everywhere. It was just unbelievable. There was no way students could go back into those residence halls.

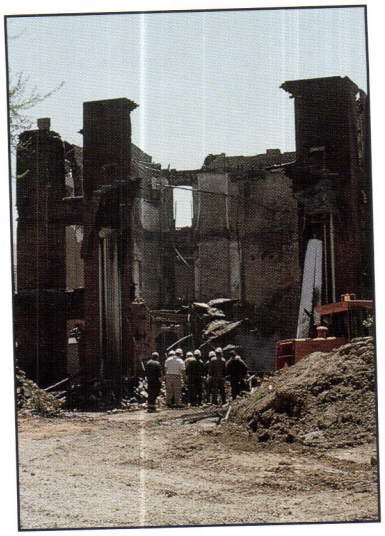
Once we decided that we were going to close the college and what actions we had to take, I called a meeting of the entire campus at 11:00 the next morning and explained to everyone what had transpired and what we were going to do. We then began the process of having students leave campus, handling all the last-minute details that had to be done.

Almost right away our insurance company brought a recovery operation to the campus, a company called Inrecon—they have 18 offices worldwide with headquarters in Michigan. They came in and began the process of recovery within 24 hours. About a day after that I had 50 people from their company living in Farmville in motels during the huge cleanup process.

Cross: One of the key goals of contingency, disaster, and emergency plans is to ensure an orderly transition and recovery if an emergency occurs. In retrospect, if you could do things differently in the planning prior to the fire, what changes would you make? What is your assessment of the plan that was in place and the

▶





The flagship of Longwood University—Ruffner Hall with its beautiful Rotunda—was completely destroyed by fire on April 24, 2001, during a major renovation. All of the historic memorabilia, including the dome paintings on the interior of the Rotunda dome, had been removed prior to the fire and will be returned to their rightful place once construction is completed in 2004. The original main Ruffner Hall and Rotunda were constructed in 1884.

execution of that plan? What communications media were used to keep the campus community informed (e-mail, voice mail, TV, campus meeting, etc.), and which was most effective?

Cormier: I don't want to sound like you can't learn anything from an event, but I would probably not have done anything differently. Please don't misinterpret that. It sounds kind of pompous, but it's not.

We had been concerned about safety and security on this campus for sometime. When I arrived in 1996, I was not here for more than one month when a reporter from the Associated Press did an expose on the lack of fire-suppression systems and sprinklers in high-rise dormitories in Virginia. I found out about this the day before Thanksgiving in 1996 with pictures of our high rises on the front page. I did not know when I came here that we did not have sprinkler systems in our high-rise dormitories. Apparently, the Commonwealth of Virginia applied a grandfather clause to these older high-rise dormitories. When I looked at our pictures in the paper, a major state paper, I asked my staff, "If I have a student on the 10th floor of my high-rise dormitory, how am I going to get her down?" When nobody could answer that, I knew we had a problem.

So from 1996 until the year 2001 this president has been very concerned about safety and security on the campus, and I have been vigilant—not only vigilant, but vociferous—and frankly uncompromising about what I expected in terms of the safety and security of our students. That's our number one concern; it's not just education. The safety and security of our students is our number one issue.

So we had been going through fire drills. We had been working as a team. We had developed a communications plan not only for this event but for all kinds of situations about how we were going to react and who was going to be there. I have a communications operation, a public relations division, that is absolutely second to none. The night of the fire every single staff person in that public relations office was with me through the night. They immediately understood what to do when we found our switchboards were overloaded and we couldn't handle all the incoming calls. We immediately got on our Web site on the Internet and started posting information and sending e-mail to various constituents.

We set up a communications center not far from the fire where people—especially the media—could call. We held a press conference. We informed every member of our Board, as I said, and the Governor and the Secretary of Education about what was occurring. We let townspeople know; we were working diligently with folks throughout this process.

So when I look at the way this campus responded, we were reacting as we said we would if such a situation should occur. You never know that you're going to lose four buildings, that they're going to explode in front of you, that you're going to have a fire that's 2,000 degrees—so hot it melted steel beams. Nobody prepares you for that. But we were prepared for what do in a crisis situation, and we already had a chain of command outlined that we followed diligently. So I would not do

things differently. The crisis management plan that was in place and the execution of that plan, in my view, were very well done. In retrospect, we did lose some contact in one of our telephone trunk lines because we didn't have an emergency generator, but that was the only thing that happened that evening that I felt we could have done differently. We now have an emergency generator.

Cross: What challenges do chancellors, presidents, and other senior leaders face in advocating for investments in disaster planning and recovery, its strategic importance, and developing sustainable funding models? On your campus, how have perceptions and attitudes changed as a result of the tragedy?

Cormier: I think that the challenge we all face is probably twofold. First of all, you don't know what life is going to bring. It is pretty unpredictable. The other challenge is that we no longer have to deal with just the natural or accidental disasters. We now have the element of terrorism. What I believe is a big challenge for leaders today is learning how to deal with the whole spectrum of disasters that your campus can encounter. Yes, there are natural disasters, but there are also other disasters. We had a situation in Virginia recently where a person came in and killed a dean, a faculty member, and a student. And then there was the sniper incident. And 9/11. These are things that you don't normally think about. But the world has changed a lot in the past few years.

It's not going to be an easy scenario as we look to the future. Our challenge is to be prepared for just about any eventuality. We recently completed a campus emergency preparedness plan for the Governor. One of the things we discovered is that you cannot put a plan together for every conceivable emergency. The way you react to a hurricane or a flood may not be quite the same reaction you're going to have to a fire or a terrorist attack. There are certain elements you can pull together for your communications plan: Who's the first person informed? Who speaks for the institution? What role does the board play? For example, we put together an emergency communications team that managed the whole recovery operation about a day after all that happened. But you have to have all of those pieces in place; you have to have that outline, that plan. So those things you can do. What is not going to be easy is preparing for every single possible situation that may occur on campus.

Cross: Public institutions throughout the United States are facing cutbacks in state funding that are causing some institutions to make major cuts in capital and operating expenditures. A review of Longwood's Web site indicates it has not been immune to these reductions, having experienced a 24-percent plus cut in state funding. What are the long- and short-term impacts of these cuts at Longwood? What has been the effect on tuition increases, contingency planning, and technology investment on campus?

Cormier: We are not going to cut safety and security. When we entered the budget process this year, we established two principles: One, we were not going to cut anything that involved the safety and security of our students; and two, we were not going to cut anything that would interfere with our core academic mission, which is teaching. Principles should guide the process. You have to know which principles are going to be sustained as you enter that process. You have to cut a budget in the same way you build a budget. When you build a budget, you say what's our core mission and how do we support that core mission?

When we faced these budget cuts, we said no interference with safety and security, no cuts in academic programs, no cuts in faculty. Now what that meant, however, was a reduction in some of the services we provide. And not only student but faculty and parent and staff services. Let me give you some examples. We had to make major cuts in housecleaning, in grounds, in several other areas within the institution, but it didn't interfere with our core academic mission. We're not having our trash emptied every day; it's emptied every other day. We've had to reduce some of what we do in terms of grounds upkeep. We've had to reduce some of what we do in our library. We had to cut back our library staff at a fairly significant level. Now you may say, isn't that partially cutting your core academic mission? Not really. Because of our campus-wide integration of technology, students still have significant access to our library collections through the Internet. It doesn't really impact significantly on what we're doing with students in the classroom. It does mean that people are going to have longer waiting times; it does mean that they're not going to get quite the services that they've had in the past.

Cross: Broadband services are estimated to be available to more than 70 percent of American households and purported by some to be capable of redefining how we work and play. What is your vision of Longwood's campus environment involving broadband services in the future? What are the *killer apps* that will spur growth at Longwood? What are the current major impediments to widespread usage in southern Virginia?

Cormier: As you probably know, we are a technology-based campus. You have to have a laptop computer to be a student here. In fact, we were one of the first institutions to require all incoming freshmen to have a laptop computer. We like to think of it as a port per pillow. That means that every

▶

student has a computer, and we're servicing about 6,000 to 7,000 computers on the campus right now. We still have some high-end user labs, and our students are fully engaged in technology. Likewise, 96 percent of our faculty are fully engaged in using technology in the classroom. In my view, technology will be essential to education in the future. I'm not convinced that technology is going to replace face-to-face teaching. I think it's going to be a tremendous enhancement to teaching, but I think there is no way that we're going to get away from the notion that people want immediate services and immediate results when they're doing their work.

Let's take the library, for example. You no longer have to go to the stacks to get what you need; you can get that from your residence hall room via the Internet. That's a very, very powerful tool. Student papers are online; we built systems here so that as you're doing your expository writing courses you can have direct access to your faculty member. You can communicate with your faculty member and your faculty member can communicate with you anytime of the night or day. Those amenities—and they're not really amenities, they're just a new way of doing our work—are going to be absolutely vital to the future. Technology will continue to progress. I believe that we're going to have to play a part in that.

I will tell you that there is a major problem in the United States when it comes to rural communities. Phone companies, Internet companies really do not want to deal with institutions or agencies or businesses that are not located near a major interstate highway. We're going to have to change that.

Another problem that we're seeing is that there's not quite the readiness for the wireless environment that we thought. We've got the wireless umbrella over the campus right now, but what we've learned, and we've tried to tell companies this, is that these firewalls can be penetrated when you're in a wireless environment. We're now trying to grapple with some of these issues. So they're not easy. Technology still has a long way to go, but we've got to understand in America that everybody has to be connected, not just those who are in major metropolitan areas.

Cross: What policy issues will the war on terrorism, expansion of law enforcement powers by the U.S. Patriot Act, and the creation of the U.S. Department of Homeland Security have on the higher-education community? As public universities, how do we balance the challenges and dilemmas of vulnerability assessment and being a good citizen while ensuring that the academy remains a forum for expression, debate, and learning?

Cormier: Really good questions. Well, the war on terrorism and the law enforcement powers of the U.S. Patriot Act and Homeland Security are already having an impact on our campuses. As you know, the new SEVIS (Student and Exchange Visitor Information System) program that they're putting into place for people who want to study in the United States is not functioning, and yet we're being forced to use these new systems for admitting foreign students on our campuses.

In addition, we just finished a major document for the Governor on emergency preparedness, and a lot of that involved terrorism. We know that these things are going to be affecting our campuses—they are already in many different ways. But you have to be careful that your basic values are not compromised. If there's anyplace in America or the world, actually, where freedom of expression can be sustained, it should be on a college campus. That means that we're going to have to be much more open about what we accept.

We all have experiences with students who have misunderstandings. We had a particular situation on our campus where some students misunderstood a Web site that was up that was, they felt, pro-Muslim and anti-Jewish. We had to have a fair number of debates on campus about that. Fortunately, we were able to resolve those, but there are all kinds of issues that are now rising up.

Our moral stance at Longwood is that this is where freedom of expression must be sustained, where we have to understand that there are going to be differences of opinion, but we have to respect those differences. It is not going to be easy to do this. We need to be cooperative, certainly, and our position as a public institution in the United States has been that we want to support homeland security; we want to support the Patriot Act; we want to support the new systems for the control of foreign students coming into the country; but that doesn't mean that we have to abandon people's freedoms as well. It is not something that is easily solved. It is going to be a campus-by-campus debate. We can learn from each other about how to get people to express themselves without being mean-spirited. But it is not going to be easy.

I am a product of World War II, and I can tell you that during WWII some pretty terrible things were said about Japanese Americans. Some pretty terrible things were said of people of German origin. I grew up on a street in New York where 17 different languages were spoken. It was not an easy time.

But this is not the first time that America has been challenged by such issues. We've been challenged from the founding of this nation. We've always had to make adjustments to the way in which we interact with other people and how we preserve our freedoms. I think we're wiser than we were during WWI and WWII. There is more tolerance in America even though one doesn't always see that. But we're going to have to work really hard at it for some time to come.

Cross: The higher-education community and society have witnessed significant gains in leveraging IT over the last 25 years. How has your campus approached crafting strategy to guide it in creating value and boosting institutional success in an uncertain world? What new and innovative projects and endeavors has Longwood implemented?

Cormier: I'm trying to frame this in the context of leveraging IT. I think technology has provided us with the democratization of information. Access to technology today is unlike anything the world has ever known. The ability of a student to communicate directly with this president, the ability of a parent to communicate directly with this president, I think, is an absolutely positive sensational opportunity for enhancing communication if it's used wisely and well.

I believe that the strategy we've crafted for Longwood is one that embraces technology without making technology a goal. Technology is a means to the end, not the end itself. That's where I think people sometimes get confused. Technology is a tool that helps us communicate in ways we could not communicate before. I've been in education for over thirty years, and I can say that this has been the most powerful, exciting time of my career. And a great deal of that is due to technology and the access we have for communicating with each other and because of the way in which we present material that we are teaching. I used to teach histology—and when I'm able to show a three-dimensional growth of a bone that I could never do on slides, that I could never do in the technology of the past, it is an absolutely marvelous opportunity. We can teach differently and better than we ever have, and I believe that we've tried to say that on our own campus.

We believe that we've been very successful and continue to be successful (if you look at our applicant pool—it's up 19 percent from the previous fall) because we're integrating technology and new forms of communication throughout the learning process. Learning is better today because of technology.

What we're most proud of is our implementation of technology within every classroom and for every student throughout the campus, and we're going to continue to work on that. We're going to try to adopt the new technologies that are emerging today into everything that we do on this campus. Our faculty and staff are very tuned in to what's happening. We're not quite the Industrial Light and Magic Company yet, but we'd like to be. It's a great time for higher education.

ACUTA thanks Dr. Cormier for taking the time to speak with us and share a look back at the fire of 2001 that devastated the Longwood campus.

▼

From the Listserve

Subject: Switch-Room Construction/Demolition

In 1996 ACUTA implemented a listserve, an e-mail-based forum that provides the ultimate venue for ongoing networking and information-sharing among members. This online discussion group is one of the most popular member benefits. Using the Web interface for the listserve, users can search discussions from the past three years by phrase or keyword and have the information listed by subject, author, or date.

The following question and two responses were posted to ACUTA's listserve in December 2002. Typical of the consistently high quality of listserve discussions, they illustrate why this resource has become so vital to so many members.

From: Carolyn S. Kane [cskane@unm.edu]

The University of New Mexico is studying the feasibility of the demolition of the telecom building, with the exception of the switch room and cable vault. A large structure would be constructed over the top of and encompassing the switch room and cable vault. Naturally, we in Telecom have some concerns.

Has anyone had experience with the successful completion of this kind of project? Any advice, comments, or information would be appreciated.

Carolyn Kane

Project/Customer Service Manager

University of New Mexico

From: Eric Fullar [efullar@uoregon.edu]

Carolyn,

Here are my thoughts, though I should add that the projects I've been involved in haven't been quite as dramatic as what you describe.

If I were in your position, I would probably start with some discussions with the engineers/architects who are writing specifications for the construction project. Make it very clear what the consequences would be if the services provided out of your switch room were interrupted for any length of time. Keep in mind that your losses would be significantly greater than the dollar value of the equipment housed in the facility.

Suppose the contractors accidentally flooded your room with five feet of water. You would need to find new equipment in a hurry and replace splices, cabling, and cross-connects as well as all of the electrical infrastructure. All of this may need to happen in a temporary facility which would either need to be wheeled in or constructed from scratch.

For even a small site, this could end up costing a great deal of money. Your contractor's standard liability insurance may just cover the cost of replacing the soggy equipment. There are disaster recovery outfits which will come in and put you back in business, but deciding who would pay for their services afterwards could get real messy.

It might be worthwhile to look into bringing in a semitrailer (or trailers) that can be set up to house and run your switch and related equipment for some period of time while your switch room is demolished and rebuilt. While this might seem an expensive option, given the time the general contractor might save in not needing to work around live equipment, it could be worth it. You'd probably need to leave cable terminations in place, but that stuff is a lot easier to enclose and leave alone while construction goes on around it. It doesn't need power, cooling, and so on.

Once you have a rough cost for the temporary facility and some idea of the repercussions of service disruptions, you (or your engineers, architects, or project managers) can go to your general contractor and say something—in writing—like, "You, the contractor, can either leave our equipment where it is or have it temporarily relocated for about this much money. The decision is yours, BUT, if you damage our equipment and/or cause any unexpected service interruptions, you will be responsible for paying (someone of your choice ... your switch vendor perhaps) to restore service as quickly as possible under our direction. You, the contractor, will also be responsible for paying hefty liquidated damages ($1,000/hour?, $10,000/hour?) that are spelled out in the specs." Then the decision is up to them; you've given them some options, constraints, and penalties to work with.

The way this approach can work is by putting enough teeth in the specs to get the general contractor's attention. Unfortunately, contractors often complain bitterly about RFPs with heavy potential liquidated damages, but they usually bid on them anyhow, especially in slow economic times.

On the bright side, you could also use this as an opportunity to make major changes to your switch room that you've been wanting for a long time ... more space, better fire suppression, water pipes re-routed somewhere other than over the top of my equipment, a new UPS, generator, more fiber-optic cable. Probably everyone in this business has thoughts that run something like, "If I had this all to do over again, I would ...."

Hope this is helpful to you. Good luck.

Eric Fullar

Univ. of Oregon Telecom Services

From: James Curtis[CurtisJ@gwm.sc.edu]

Well, you kind of said it all, Eric.

One point I would make is to ensure that the new switch room has redundant feeds or at least redundant pathing for "Bell" service ... We have just gone through that with everything live, and it was an interesting experience since we share the computer floor with the mainframe and server farms.

Also, I would look at cleaning up all the backboards and feed cables and going to overhead cabling. We did that on our upgrade to get out from under the floor and get some control of the wiring. (Here again we are sharing space with multiple entities, who are not necessarily careful of other people's cables under the floor.)

I strongly concur with Eric's comments and would recommend relocation of the primary service to an alternate location. You cannot afford the down time if they cut the wrong cables, etc.

One other thing I would recommend, if you do not already have one, is a little "test" area where you can test different types of phones, an outside line or two, and consolidation of any call-accounting, agent-accounting hardware/software into that same area. We have done that with great success.

Jim Curtis
Operations Manager, Communications
University of South Carolina

Guide to IT/Telecom Disaster-Recovery and Business-Continuity Planning

by Steve J. Hailey

In this post-September 11 environment, disaster recovery/business continuity and the challenges associated with communications during a catastrophic event have been in the spotlight in the IT and telecommunications industry. New technologies have brought both creative innovations and unique challenges to the disaster-recovery process.

For example, as organizations move into converged voice and data networks with endpoint locations virtually anywhere, E-911 services become increasingly more difficult. A network configured improperly hampers the efforts of campus public safety and 911 responders to effectively locate the party who dialed 911. However, converged voice and data networks that include IP telephony now allow for backups and redundancies that were never available before.

Some simple step-by-step processes will start you and your institution on the right path to a successful IT/telecom disaster-recovery and business-continuity plan.

The Goals of Planning

Planning starts with prevention. Devise checklists that will help you assess the level of risk and compare current practices to best practices. Develop specific steps for reducing the risk of an outage as well as restoring operations should an outage occur. Prioritize those deficiencies you identify to ensure adequate controls are implemented.

Having said that, the primary objective of any disaster plan is to enable an organization to survive and to continue normal business operations. Throughout the recovery effort, having a plan establishes clear lines of authority and prioritizes work efforts.

An effective plan will include the following key objectives:

- Provide for the safety and well-being of people on the premises
- Minimize immediate damage and losses
- Establish management succession and emergency powers
- Continue critical business operations
- Facilitate effective coordination of recovery tasks
- Minimize the duration of a serious disruption to operations and resources (both information-processing and other resources)
- Reduce the complexity of the recovery effort

Planning Process

The planning process should fully describe developmental tasks, present planning scenarios, identify resource requirements, and designate and provide direction for management and project teams.

Developmental tasks will include the following:

- Initial assessment
- Project manager and team selection
- Process development
- Documentation

Potential scenarios must be considered, such as:

- System unavailable for more than 24 hours

- Data corrupted or cannot be accessed
- Facility damage/loss of personnel
- Temporary closure of the facility
- Facility used as a public shelter

Resource requirements include key personnel:

- An executive sponsor who ensures management commitment
- A project manager who is aware of strategic objectives of the institution and familiar with operations of all business units, has project management and audit experience, has written and verbal communication and facilitation skills, and is detail oriented.

Assign available staff to various management teams, including:

- Crisis management
- Business continuity management
- Emergency response
- Special purpose and business unit
- Executive management/middle management
- First response

The actual project team should include an advisory group that reviews recommended processes and forms before business-unit team leader meetings. Its members are the business continuity management team leader, an IT representative, and a facilities/risk-management representative.

Recovery Planning Tasks

Being prepared to respond in the event of a disaster requires the steps described here:

1. Project planning: First you must have a process in place to define the project scope, organize the project, and identify the resources needed.
2. Critical business requirements: Not only must you identify the business functions most important to protect and the means to protect them, you must also analyze risks, threats, and vulnerabilities.
3. Recovery strategy: Arrange for alternate processing facilities to use during a disaster. Make sure you store copies of computer files, work-in-process, software, and documentation in a safe place—off-site, if feasible.
4. Emergency response/problem escalation: Specify exactly how to respond to emergencies and how to tell when a problem has become a potential disaster.
5. Plan activation: Determine procedures for informing the right people, assessing the impact on operations, and starting the recovery efforts.
6. Training: Make sure everyone understands the recovery plan and can carry it out effectively.
7. Testing and maintenance: Conduct annual, quarterly, and monthly reviews of key components to ensure timely updates of the plan. Test all phases in all business units each year, and schedule after-action reviews after an incident.

Disaster-recovery planning is not a two-month project; neither is it a project that can be completed and forgotten. An effective recovery plan is a living recovery plan. The plan must be maintained to remain current and must be tested regularly.

Outside Services Are Available

A variety of vendors have services and solutions designed to assist you with your IT/telecom disaster-recovery planning process. Some of the solutions available include:

- Network emergency preparedness assessments designed to help you review your current voice and data environment, discover and prioritize gaps, and ensure proper redundancies and backups are in place.
- Mobile communications networks, customized solutions designed around your specific requirements and tailored to fit your needs.
- Emergency notification solutions that are built around your specific requirements and allow you to focus on the situation at hand rather than on message delivery.
- Priority-based emergency communication, an application that enables multilevel precedence and preemption (MLPP) on your enterprise PBX and can provide your critical personnel with the ability to dial a special code to allow priority outbound calling during times of network overload.
- Speech-based security solutions, including speech biometrics applications that, combined with PIN codes for maximum effectiveness, provide data-access security and identity verification.
- Premise-telecom service priority in which some vendors provide you 24/7 assurance that your premise equipment and related applications will be restored under a plan that gives you peace of mind should an unforeseen event result in down-time.

Where Do We Go from Here?

In today's world it is important to avoid trying to reinvent business, choosing rather to rethink the way we do business. The goal is to leverage new and existing technologies to help your organization prepare, respond, and recover from any day-to-day emergency or a major catastrophic event.

Steve J. Hailey spent more than 10 years at the American Red Cross - National Headquarters working for disaster telecommunications. He is now an account executive/project engineer for Daycom Systems Inc., specializing in IT/Telecom Disaster-Recovery and Business-Continuity Planning. He can be reached at steveh@daycomsystems.com.

▼

Lessons Learned: Looking Back on Disaster

by Rich Lehn
Charles Wall
Jack Canavera
and Linda Hosey

No one wants to believe that they may be the next to experience disaster firsthand, but we all know that calamity, wearing any one of many faces, may strike at any time. Following are comments from four ACUTA members who found themselves unexpectedly in the middle of a crisis and some sound advice they offer in retrospect.

Rich Lehn, University of North Dakota

In April, 1997, the University of North Dakota Telecommunications Department played a pivotal role in providing telecommunication services for the university and the community of Grand Forks during a catastrophic flood and the weeks following. Staff were onsite 24 hours a day for nine days and for extended hours after that. They performed a variety of extraordinary tasks such as pumping water from the main cable vault, cable manholes, and nearby steam tunnels in hopes of staying ahead of the water levels and protecting the telephone system. Several campus buildings as well as many homes and businesses were destroyed, the city was evacuated, and many people were without power for weeks.

While your campus may have a disaster plan in place, chances are the situation you find yourself in will not have been covered. You will need to "think on your feet" to get the job done. Here are some thoughts that may help you in a disaster, based on my experience with the flood of 1997.

1. In creating a disaster plan, include a list of possible locations to which your staff may go should they evacuate your community. Who could you contact to make sure your staff members are okay, to keep them updated, and to notify them when the work area reopens?

2. Major disasters leave people working in very dangerous and unhealthy conditions. Long hours plus cold, wet, and otherwise miserable conditions increase the likelihood of accidents. Working in pairs or teams helps reduce the possibility of accidents and, should something serious happen, another person is there to help or call for help.

3. You may find very little to work with the first few days after a major disaster. Safety becomes a major concern. Your situation may include no medical facilities, no potable water, no municipal gas supply for heat or fuel for generators, and no electricity. Plan now how you will deal with these issues.

4. Keep a journal of what was done and when so you can go back and recreate events that took place. This will also assist you in undoing things you did just because they were needed at the time.

5. Whenever possible, and especially during the recovery phase, contract for work that needs to be done instead of having your staff do it. This frees up your staff to deal with issues of their own, plus you will have simplified your life for future dealings with FEMA and insurance companies. In my experience, FEMA would only cover the

employee's actual salary and materials used at cost. Overhead and depreciation expenses that would normally be part of the operation's hourly charge could not be claimed. A contractor's invoice for doing this work, however, was rarely questioned.

At the time of a disaster, things appear very bleak. They do get better, and you must keep the faith.

Charles Wall, Austin Peay State University

In the pre-dawn hours of January 22, 1999, a tornado struck Clarksville, Tennessee. While no one was seriously injured, property damage was extensive. Located directly in the path of the storm, the campus of Austin Peay State University was hit full force. Virtually all of the 30-plus buildings on the main campus suffered damage. Five buildings suffered major damage; and three of these, including a dormitory, were closed for months.

The office of Information Technology had a formal disaster recovery plan. However, the plan was not specific to the type of damage we sustained, and much of our response was based on making the best decisions possible on the scene. In the months following the damage, we reflected both informally and formally with state auditors concerning our experiences. Based on my recollections, I offer the following comments:

1. Many agencies are willing and able to help as time goes by, but during the initial minutes, hours, and maybe even days, you are pretty much on your own. Know what resources you have available. This includes not only equipment and supplies but human resources as well. Be creative, and assign tasks to individuals who will get things done without direct supervision, particularly during the initial response. As a formal plan of action develops, operate within that structure—but don't sit around waiting to get started.

2. Don't count on normal communication channels to function. Have alternatives. Our primary mission for IT was to maintain communications for the campus. We arranged for emergency generators to power telephone and computer equipment as well as the campus radio repeater system. Cell-phone service was severely overloaded. We had access to cell phones from two major providers, but it was not unusual for both systems to be saturated. If communication channels are adequate, staff members living outside the damaged area can be valuable resources to contact other staff members and provide a communication post. Once we got our computer equipment back online, we used the Web to communicate with students, faculty, and staff regarding our recovery efforts and plans to reopen school.

3. Our telephone switch and computer room had several hours of battery backup but no emergency generator. As a result of this experience, we now have a generator capable of powering the administration building—including both the telephone switch and computer room—for extended periods.

We used small portable generators initially to bring up a small telephone switch in our emergency operations center and for our radio repeaters. Generators also provided enough power for our cafeteria to feed the students living on campus as well as staff and other emergency workers. A much larger generator capable of powering the entire administration building, secured from the National Guard, arrived late in the first day. Commercial power was not fully restored for several days.

4. Staff members may have trouble reaching the site and should be prepared for long work days, including the possibility of living on the job. In our case, the first responders had to deal with debris, downed trees, and downed power lines in order to get in.

Others who tried to come in later had to deal with a variety of different law enforcement agencies responsible for keeping people out of the damaged areas. A number of truly dedicated souls found side streets that were not yet patrolled and were able to get in. Once they got in, they could not count on getting out and then back in, even when on a mission to purchase emergency supplies from vendors located in areas outside the damaged area.

Our campus police worked with the other law enforcement agencies and tried to clear admission for those who were working. When I arrived approximately 30 minutes after the storm hit, I had to work around debris in the dark to reach campus, and I only passed through one police check point. By the third day, a number of other agencies were providing supplemental security, and I had more trouble getting past a park ranger who had been assigned to keep nonessential personnel off our campus. A two-way radio on the campus police frequency allowed me to get a message relayed to the officer, and I got in.

5. Be prepared to deal with small annoyances such as flat tires. Streets were covered with debris that included glass and nails from the many roof shingles that were everywhere. Our Physical Plant people repaired tires on institution-owned vehicles for weeks following the tornado.

Jack Canavera, St. Louis Comm. College

One afternoon in October 1997, just outside the main building of SLCC's Forest Park campus, an eight-inch water main broke. Water broke through the foundation wall, flooding and sending debris through the two lower basement levels of the campus. The fire department sent pumper trucks to control the rising water, but unfortunately, no one knew that the main valve was buried under three

▶

inches of asphalt in the road outside the campus. The water was not shut off until 8:30 that evening. For hours, the water continued to rise, and SLCC's switch room took in about five feet of water.

Here are some of the lessons we learned:

1. Consider water utility shut-off points. Do not depend upon your utility supplier's valves to be the only source of shut-offs to your campus.

2. Don't allow high-level administration to allocate limited land-line resources to high-level officials only. Remember the worker bees who keep us in business. Give officialdom cellular equipment.

3. Have written agreements ready to sign for those users using borrowed equipment. Consider usage, treatment of equipment, instruction manuals, boxes, and more.

4. Keep a copy of your system programming, documentation, and other relevant information offsite. If you think your maintenance provider has this information, ask to see it or inquire about its whereabouts.

5. If you are DID oriented, how will calls be handled if you are using a temporary system or a system with limited facilities?

6. Can you automate the process of information distribution rather than taking personal calls? Remember lots of people will call wanting additional information.

7. Remember that if you need to replace your PBX, your costs may be higher than expected depending upon your manufacturer's policies. In some cases your PBX software may be "married" to the PBX that is damaged and may need to be purchased again.

8. Don't do your initial assessment of damage without a representative of your insurance company present.

9. Review your insurance regarding repair and replacement issues. Replacement coverage may also mean repair or purchase of remanufactured equipment which could affect compatibility with other equipment.

10. Understand that your urgency to replace your equipment may require you to expend funds with no guarantee of insurance coverage.

11. Consider the procedures necessary to make major expenditures during an emergency. If you are a public entity, can you modify bid procedures and processes to expedite your recovery?

12. Consider union issues. With rapid recovery a priority, you may need to remember the various union affiliations (or lack thereof) of the outside vendors who will be working at your site.

13. Consider security, not only of the affected site, but also of command centers. Look out for press being present at meetings where vendors (unfamiliar faces) are present.

After this disaster occurred, SLCC sued the City of St. Louis for the damages caused by the failure to find the main shut-off valve which had been paved over in the street fronting the Forest Park campus. The suit was settled with the City (or their insurers) paying the cost of the extraordinary damages caused by the delay in finding the shut-off.

Shortly after our flood at Forest Park, new external shut-off valves were installed on college property for the water lines feeding each of our three campuses. We also relocated the switch room out of the basement.

Linda Hosey, University of Maryland

On the afternoon of Monday, September 24, 2001, a tornado struck the University of Maryland at College Park. Two students lost their lives; a number of students, faculty, and staff were injured; and a large number of students were left temporarily homeless due to damage sustained by their dormitories and apartments. The total cost of the damage to property exceeded $15 million.

Prior to September 2001, we believed we were very good at planning for and handling many types of emergencies. The university has now been introduced to a whole new set of potential disasters that were previously inconceivable, including not just natural disasters but terrorism as well. As a result, the Public Safety Operations Committee has directed increased attention and resources to emergency planning.

OIT's Networking and Telecommunications Services is actively involved in exploring ways in which the university's communications systems and contingency systems can be secured as well as accessed in the event of an emergency. Emphasis is being placed on the prevention of incidents, contingency planning, resolution during incidents, and recovery.

Some specific areas in which NTS is actively focusing include the following:

- identification of potential threats
- prevention/resolution/recovery plans
- offsite storage of communication system data
- identification of essential services which must be maintained during emergencies
- essential personnel issues
- building security
- vendor requirements and options for utilizing vendor resources in emergencies
- redundant equipment and routing to ensure continuous operations
- special remote access provisions should operations need to be handled remotely
- coordination plans with other departments
- documentation of critical data in various media such as disk, paper, and electronic; and recovery approach options

Thanks to these members for sharing their experiences. Reach them at the following e-mails: Rich Lehn, rich_lehn@operations.und.edu; Charles Wall, wallc@apsu.edu;Jack Canavera, jcanavera@stlcc.edu; Linda Hosey, linda@nts.umd.edu.

Get Your Data Network Ready for Voice

by Jay R. Brandstadter

Despite the economic blues and distress in the telecom industry, interest in IP–based enterprise phone systems (IP-PBXs) is expanding rapidly. Although there is reason to question whether the complex array of voice over IP (VoIP) technologies and products is fully ready and whether these technologies and products offer a compelling value proposition for the user community, all PBX vendors are now delivering VoIP or IP telephony systems. Many users in higher education are doing trials, network analysis, or operational deployments—and many more are trying to decide whether and how VoIP can benefit their institution. *(See sidebar on page 38 for one such example.)*

However, the fact that IP networks can carry voice doesn't mean that all IP networks will do it with acceptable reliability and quality. Many VoIP installations fail—or run up large unbudgeted expenses—because the LAN, WAN, or both are unable to handle voice successfully due to needed infrastructure and other changes. Customers often overlook, and vendors often downplay, the need to ensure that the data network is up to the challenge of voice.

If your institution is considering VoIP, you must know whether your data networks are voice-ready. If the proposed installation will compromise call quality, it's essential to know that in advance—so you can decide either that reduced quality is acceptable for your application or that you need and can afford an upgrade.

Start with Inventory and a Plan

Suppose your institution has approved some sort of initial step toward convergence of the voice and data networks. You're probably going to start migrating to VoIP through a pilot project in a portion or subnetwork of your data network infrastructure and then expand the rollout over time, based on results, budget, and other factors. Interoperability between your IP-based system and legacy voice networks could be a big problem, especially if you are mixing vendors.

Selecting the initial data network for migration to VoIP is not a trivial matter. If you're fortunate to have latitude in that decision, you should opt for a controlled or bounded situation, preferably a new or *greenfield* site or infrastructure. If you're not that lucky, then you'll have to upgrade an in-place data network for voice.

You will need to assemble traffic data for the voice calls running over this network, decide on a method of digitizing and compressing the voice signals, and convert this information into estimated bandwidth requirements.

Taking Stock

Start by taking stock of your data network assets and develop a road map or plan of where you want to go. You ▶

will have to learn everything you can about the network: configuration, equipment, data traffic, applications, users, interfaces, bandwidth/capacity, performance characteristics, error rates, and so on.

You will need to assess growth for the network—not only through the addition of voice but also for video, fax, Web interaction, and other media and applications. LANs and WANs pose different challenges for VoIP and must be analyzed separately.

As part of this initial assessment, the relationship between potential voice applications and the data network needs to be considered. (*Voice* should be defined to include related applications, such as voice mail/messaging and voice-activated processes.) This relationship defines some boundary conditions on numerous aspects of a converged solution.

For example, how do the server requirements of the voice portion affect the IP network's configuration and bandwidth? What cooperative, interoperable functions and mechanisms are feasible in a multivendor architecture, where, for example, PBXs or voice servers are from different vendors than routers and data switches? How can the data network be strengthened to provide the comfort and robustness of familiar legacy voice and voice-related capabilities?

The Perils of Packets

Packetizing voice for transmission and handling by IP networks makes significant demands on the network. Packetizing generally begins with digitization and compression of the voice signal by a CODEC using a standard like G.711 or G.729.

VoIP at UTHSC

Hardy Kail
University of Texas Health Science Center
San Antonio, Texas

In the summer of 2000 we purchased the NEC IP Gateway product to begin some testing with VoIP. To test the voice quality we installed IP adaptors on three existing telephones used by the technical support staff as their primary telephones. These telephones have been in constant operation since August 2000, and at no time has anyone on the far end of a conversation complained of poor voice quality.

After the initial tests, we decided to expand the scope test from wide area network (WAN) locations. We first installed telephones in our homes on cable modem and DSL services. The voice quality was the same as on campus; however, since these connections had no QoS capability, there was occasional clipping, especially during the Napster era. These telephones are still used today by telecommuters and for voice-network troubleshooting.

After hours we receive either equipment or circuit alarms for our remote sites. With the VoIP telephone we are able to make an on-network call to an on-site security person or to place a voice call into a communications room and listen for alarms, radios, or air conditioning noise. We have avoided several late-night or weekend trips by testing from home.

In the summer of 2001 we started having some congestion on our existing trunking between some remote sites that had both voice and data capability. We needed to expand trunking capability, but that would require additional circuits and additional monthly recurring charges. We decided to install VoIP trunking between two NEAX 2400 IPX sites and one NEAX IVS 2000 system in order to utilize the existing bandwidth for both voice and data. We set the voice routing to use the VoIP trunking as first-choice calling to and from each of the sites. There have been no reports of voice issues, plus our call-blocking problems at these sites no longer occur. We are in the process of adding a fourth site to this configuration in the first quarter of 2003 at a location 250 miles from our main campus.

Another project is the opening of our first off-campus office with all IP telephones in February. We are also in the process of developing a disaster-recovery plan around a PBX supporting 100 percent VoIP telephones.

Users are accustomed to phone conversations with *toll-quality* sound and performance. Getting that quality over a data network is far from guaranteed. In a traditional voice network, every call is assured a fixed amount of bandwidth; in an IP network, voice packets must contend for network resources with other traffic using the system—and the amount of contention varies millisecond by millisecond.

As a result, packets can be delayed (latency), the amount of packet delay may vary (jitter), packets are lost or dropped, and some arrive out of sequence. Beyond a certain level, all these problems degrade voice quality and can even cause dropped calls. These problems can essentially be eliminated, but ultimately it's a matter of aural perception.

Formula for Trouble

These problems don't just affect human-to-human communication. Other calls that can use VoIP connections—most notably dial-up modem and fax calls—are particularly sensitive to dropped packets. In such cases, losing a packet or two will generally drop the call.

Even with Gigabit Ethernet LAN backbones and switched 100 Mbps to the desktop, you cannot ignore the potential for trouble. Consider an e-mail with a long attachment (e.g., a large PowerPoint file) that is broadcast to most of the users on a corporate LAN. Now try to get even a normal volume of LAN telephony calls through at that moment. Any questions?

The amount of damage caused by these packet perils is, of course, closely tied to the available bandwidth and the nature and volume of the traffic handled by the IP network. As traffic increases, packets may enter the network faster than they can be forwarded, causing congestion. Data and video such as streaming IP video in distance-learning applications will, of course, add to the traffic load. When the network or network segment approaches a congested state, packet delay increases, packets may be dropped, and the network appears to slow down.

There are numerous tradeoffs between key measures that affect voice quality (delay, jitter, and packet loss), bandwidth, network architecture, and network policies. These are complex relationships marked by a delicate balance among many factors and parameters.

Navigating these waters to provide voice on a data network is no simple matter, but you can begin by examining how to tune the data network and whether to employ quality of service (QoS) policies.

Tuning

IP-PBX providers and integrators will assess your data network's voice readiness—often for a price—or you can do it on your own using network assessment tools of providers such as NetIQ. Once you determine that some degree of upgrade is required, you can take a number of measures to improve call quality.

You can add more bandwidth, upgrade or replace existing network equipment, improve your network architecture, or reconfigure the network. Bandwidth can be made available by acquiring higher-speed links—more expensive in the WAN than the LAN—and by more efficient use of the bandwidth available. Options in the latter category include increasing voice compression, varying ▶

Network-Upgrade Cost Elements

Upgrading a data network for voice can involve several different types of expenditures. Here are some cost elements to consider.

Network Upgrades (independent of QoS)

- Acquisition of new and/or higher-speed links
- Replacement or upgrade of switches/routers (including software)
- Reengineering of network configuration

Additional Network Upgrades for QoS

Reliability/Availability Upgrades

- Redundancy in switches/routers and links
- Failover/backup to public network
- Uninterruptible power supply

Security Upgrades

- Update of firewalls and other software-based security measures to hardware solutions to reduce processing delays
- Other upgrades or replacements to provide legacy voice security capabilities

Network Management Upgrades

- Upgrade management system to support voice and data network with QoS

Support, Training, and Learning

- Training on convergence and voice/data cross-training
- Acquisition of VoIP-capable staff and consultant support
- Experimentation with pilot or other proof-of-concept tests

packet size and framing, using silence suppression and voice-activity detection, and compressing the RTP headers of packets. These methods try to minimize packet overhead and maximize the efficiency of packet payload.

There are lots of trade-offs here. For example, using lower data-rate CODECs for voice compression will save bandwidth but may reduce voice quality below the level required for your application. An alternative approach may be to use call-admissions control software that limits the number of concurrent VoIP conversations to an acceptable predefined number, overflowing additional calls to a non-IP network.

It is also possible to improve performance and capacity without buying more or bigger pipes by upgrading or replacing network equipment. Among the available techniques are the following:

- Assure that you have up-to-date high-speed switches and no hubs in LANs.
- Replace software-based processes or functions (e.g., firewalls) with hardware-based versions to reduce delay times and increase capacities.
- Increase memory (RAM) for router queues and other traffic-sensitive points in the system.
- Assess whether your network backbone switches/routers are in need of modernization or upgrade to meet the new voice requirements.

Also, a review of the network layout and architecture can be helpful. Can shorter, more direct routes be established for VoIP calls, thus reducing propagation and transport delays? Can the number of router hops be reduced? Will a better understanding of traffic patterns or "communities of interest" lead to improved network performance?

Quality of Service

Another way to use the data network more efficiently is to create different categories or classes of traffic and give priority to some categories over others. This approach, generally called quality of service (QoS), does not eliminate congestion, but it allows traffic to be prioritized so that the traffic most sensitive to delay goes to the front of the line.

There are differing opinions on whether a QoS mechanism is essential to a successful VoIP installation. It's often argued (especially by data-centric vendors) that assigning priority to every voice packet is the only way to be sure that voice will get through.

Others (including some traditional PBX makers) point out that when the data network is less than cutting-edge and operates in mixed-vendor environments, QoS may be prohibitively expensive. Here, incremental improvements to bandwidth and equipment, particularly in the LAN, may provide an effective and less costly solution.

There are certainly examples of VoIP installations that have achieved acceptable call quality without QoS, simply by throwing more bandwidth at the congestion problem. Increasingly, vendors are including QoS technology in their LAN switches at no extra cost, giving users the option to turn it on. But upgrading to such equipment isn't free—nor is the management software needed to control and monitor it.

Most seriously, in QoS, vendors generally *talk the talk* of open standards but *walk the walk* of proprietary technology— which means that QoS just doesn't work very well in multi-vendor environments. If all your networking gear carries one vendor's logo, QoS can be an elegant, though still complex and time-consuming, solution. Otherwise, it's yet another immature technology associated with VoIP—implying frequent changes, and possibly inadequate knowledge, experience, and tools.

Keeping Track of Costs

If the new IP-based phone systems are to be a viable alternative to circuit-switched voice, they must reproduce the comfort, robustness, and overall familiarity of legacy voice systems and the public switched network. The system must offer the network owner and network engineer reliability, security, manageability, and availability of qualified support people and tools. Right now these items are primarily works-in-progress.

Tuning and QoS mechanisms will help prepare data infrastructures to support voice, but they aren't free. The box on this page presents a checklist of some major components in readying a data network for voice. This cost summary profile is not intended to deter you from considering VoIP for your organization. It does highlight, however, that there are many potential data-network costs that need to be factored into your VoIP value proposition.

Training, education, and conferences on convergence and VoIP are available from numerous sources, and the topic is beginning to appear in industry publications. PBX makers, independent vendors, and telecom consultants can all offer help, but at this point everyone is still in learning mode.

Conclusion

Is it still too early to enter the shark-infested waters of VoIP migration? Not necessarily. But be patient and do your homework as best you can. The readiness of data networks to support voice is a moot point if your organization is not prepared and the payback is not clear. Think of the complexities and the machinations needed for the data infrastructure to handle voice, which the circuit-switched world has been doing quite well for decades, and calculate carefully whether beginning this transition now is beneficial.

Jay R. Brandstadter is a partner of Delphi, Inc., a Washington, D.C.-based consulting firm. He can be contacted at 301/871-1021 or *jbrand@rcn.com*.

▼

The Voice-Data Culture Clash

The readiness of the data network to support voice includes the voice-data readiness of the people that make it happen and maintain it. Unfortunately, voice and data people speak different languages.

Consider the following points from a recent Cisco presentation on VoIP:

1. Use Differentiated Services or IP Precedence (IETF RFC 2474) on all WAN interfaces in a Voice over Data Network Voice (DSCP=EF), Video (DSCP=AF410), Voice/Video Call Control (DSCP=AF31).
2. Use MLPPP LFI (RFC 1990) or FRF.12 on WAN connections below 768 Kbps.

If you are familiar with wide-area data network standards, that makes perfect sense. Otherwise, it's a foreign language. Voice jargon can be just as confusing to data folks. What on earth are DTMF, ADPCM, and PRI?

The language differences are but one aspect of the culture clashes that come into play when voice and data are merged. How are the voice people to learn enough about data to work effectively with VoIP? Conversely, data network folks need to know and be sensitized to voice and its unique characteristics. Can you hire people with appropriate knowledge in both disciplines? Where can you get voice-data training?

Don't count on your vendors and system suppliers to assist you in that training. They themselves may be still in the process of assembling the skills needed to break down language and other barriers between voice and data.

There is a scarcity of IT staff today with combined voice and data skills. Even if VoIP will ultimately permit a reduction in support staff, the potential benefit may be offset by the difficulty and cost of finding and keeping staff with combined voice and data expertise.

INSTITUTIONAL EXCELLENCE IN TELECOMMUNICATIONS AWARD 2002

Berklee College of Music

by David Lustig

With a matriculated population of 3,100 FTE, Berklee College of Music is the largest independent college of music in the world. Located in the Back Bay area of Boston, Berklee was founded on two core ideals: that music could be taught through studying the music of the moment and that our students need practical, professional skills for successful, sustainable music careers.

For more than 50 years, we've demonstrated our commitment to musical currency by wholeheartedly embracing change. We adapt our curriculum to make it more relevant, upgrade our technology, and attract diverse students who reflect the multiplicity of influences in today's music. We develop new initiatives to reach and influence an ever-widening audience. Berklee's use of videoconferencing technologies in support of distance learning is one such initiative.

Description of Endeavor

Berklee uses videoconferencing technology as a transmission medium for distance education in music. We set up small, inexpensive, temporary television studios on either side of a connection and use the equipment to provide opportunities to our students, alumni, and the students of our Berklee International Network (BIN) partners that would otherwise be impossible or impractical. Although the studios we set up typically have high-quality sound systems and two or three cameras, we also produce events that use single-camera units when the situation allows. Our initiative's mission, after all, is to explore ways and means of providing excellent music education through distance learning.

Berklee's unique partnerships with the BIN members in 14 countries and our alumni around the world as well as many music business and performance organizations mean that our students and alumni can receive *just-in-time* education that's as relevant and current to them as the music they play.

We integrate video and audio systems into our videoconference units through existing video switcher and audio mixer technology. We use the videoconferencing system's audio compression and echo-cancelling circuitry through its normal auxiliary input port. Video input is handled similarly, through the second camera input connector. We use the built-in camera when appropriate, too. For example, a single virtual visiting lecturer can often be accommodated by a single camera and the videoconference unit's built-in microphone. Our events have received press coverage through the Associated Press as well as through electronic media in the United States and abroad.

Planning, Leadership, and Management Support

Berklee's planning process for a summit of all BIN members in Athens, Greece, identified the problem of including as many participants from Berklee's

campus in Boston as possible. A team that included Berklee's executive vice president, vice presidents for IT and institutional advancement, associate vice presidents for operations and for international and special programs, and the assistant vice presidents for IT and special programs considered this problem. Our team rapidly concluded that videoconferenc-ing technology would be an excellent way to involve as many Boston participants as possible in this important biennial event. We then proposed a number of demonstration music classes so we could explore various modes of learning and music using this medium. Our provost enthusiastically endorsed the concept, rounding out executive support of the project.

From the beginning, a large number of staff were involved so that our development time would be minimized, while maximizing institutional learning. The staff was from Academic Affairs; the Departments of Information Technology, International Programs, and Special Programs; the Office of the President; and the Nakas Conservatory of Athens.

The assistant vice presidents for special programs and IT led the planning for each individual videoconference, which we termed an *event.* The planning for each event included a script. A master schedule detailed all events, technical trials, and rehearsals.

Promotion of Technology and Maturity of Effort

At Berklee, we stress the use of commercially available technologies. We use ISDN circuits to support videoconferencing because the circuits are available worldwide. So, too, are videoconferencing systems that comply with the H.320 standard. Operating at 512 Kbps permits excellent sound quality and very good video, although operation at 384 Kbps is acceptable as a fallback during events.

We set out to use videoconferencing in the support of music and music education, not merely to do something different. As it turns out, partners and media have informed us that indeed, the musical and educational collaboration we've demonstrated is unique.

Our successful experiences from the May 2000 demonstration events led to the installation of three Lucent 6000 ISDN switches, which support up to three simultaneous 512-Kbps videoconferences each. These switches are installed to provide access to digital bandwidth from key classrooms, conference rooms, performance venues, and recording studios at Berklee.

Our academic colleagues are excited about the opportunities available through this medium. Gary Burton, our executive vice president and five-time Grammy Award winner, hosted a virtual visiting artist session on composition featuring Greek composer Thanos Microutsikos from Greece to Boston on November 2, 2001, and a virtual master class on improvisation technique to Berklee alumni in Los Angeles from Boston on November 18, 2001. Berklee professor John Pierce has taught jazz improvisation to a class in Athens. Instructors in music composition, music business, and music technology plan to incorporate virtual guest lecturers in their syllabi for coming semesters.

Quality, Performance, and Productivity Measurement

In music education, sound quality is of primary importance. In master class situations, critical music performance technique must be visible at the far end. Fortunately, videoconferencing at 384 Kbps is acceptable, and 512 Kbps supports our objectives well.

Our instructors are key assessors of our efforts, as are students, administrators, and technicians. For assessment purposes, each session is recorded from the perspective of both ends of the circuit—source and target. In addition, we have used separate camera crews to record the activities behind the scenes of many of our events so that we can study and improve our teaching and presentation techniques.

Professor John Pierce is analyzing and reviewing student participation in his improvisation class by digitizing segments of the class and putting the segments and his comments on the Web for his Greek students. In this manner, students can view their work and John's comments at their own pace and participate more fully in the videoconferenced events.

Berklee's measurement criteria are very pragmatic: Are music and music education served? To respond, we use our videotapes from sessions to determine student interest and attention. We can, of course, empirically observe improvement in playing and improvisation skills. Our alumni responded very favorably to the sessions we have hosted for their benefit as evidence by increased attendance. Instructors modify their syllabi to accommodate the new medium. From all indications, all

▶

participants are eager to take advantage of our capabilities—technicians, educators, guest lecturers, administrators, students, alumni, partners, and parents.

Cost, Benefit, and Risk Analysis

The cost of entry is surprisingly small. ISDN Basic Rate Interface (BRI) circuits cost about $30 per month. We use four circuits to support 512-Kbps transmissions. We use twenty cents per Bearer Channel (B Channel) connection per minute as our working estimate for domestic-event line charges. For international events, we budget two dollars per B Channel per minute. Even though these estimates are admittedly on the high side, they provide a conservative estimate for comparison to site visits.

We typically budget three times an event's run length for testing, rehearsals, the event, and assessment videoconferences. In other words, we would budget three hours of time online for a one-hour event. Domestically, that equals $288 or $2,880 for international events. We find that compared with the cost and lost opportunity of asking personnel to travel two days and be onsite for one day as opposed to a three-hour total investment, videoconferencing pays for itself quickly!

The hardware used for BRI connectivity is readily available. Units of the type that Berklee uses cost about $8,000 domestically and $10,000 internationally.

As all of our technologies are off-the-shelf, Berklee benefits from the maturity of the technologies it uses. We can choose at which point on the maturity/cost/ubiquity scale we implement technologies. This freedom of choice gives us terrific flexibility and growth opportunities.

Customer Satisfaction and Results to Date

Berklee's motto, *esse quam videri,* is generally translated as "to be, rather than to seem to be." We find that in music, success and failure are easily discernible. So are our efforts in applying technology to music education.

At the outset, we perceived that our community would respond favorably to any technology that would improve musicianship either as individuals or as a community, music being a highly collaborative endeavor. The perception was correct. Our community has responded enthusiastically, as measured by attendance at events and by the increasing number of events requested.

Coming on the heels of the improvisation class hosted by John Pierce was a guitar virtual master class during Guitar Week at the Nakas Conservatory by Jim Kelly. At the 2002 BIN Summit in Boston, we took an entire day teaching our international partner schools technical and pedagogical techniques that they were able to apply at their home institutions. We taught them by having three teams each produce a 15-minute videoconference and present it to the rest of the summit attendees. Everyone received a DVD containing the resultant presentations.

Next was a class hosted by the Nakas Conservatory to Berklee on Greek percussion and rhythm. The classes we offer in international music became much richer with the addition of expert practitioners coming directly from their homelands to our students in Boston. Our corporate partners have taken notice, too. In October 2000, Berklee and Apple Computer sponsored a one-day workshop on technology in music education. The event was webcast through Akamai Technologies, and during the day we hosted the electronic jazz ensemble of Hilltop High School of Chula Vista, California, via videoconferencing. This, too, was included in the webcast.

Conclusion

Dropped lines, late equipment arrival, incomplete facilities, and the learning curve of the new medium have all caused us to regroup and rethink approaches in the past three years. We can now provide guidance to our educators, technical staff, and partners so that their learning curves are graceful and productive.

Music is an art form of continual, consistent improvement. Berklee's approach to technology in music and music education mirrors this perspective. Each event, every participant, and every technician involved in our initiative contributes to the effort. In our initiative as in our art, the presentation of participants' perspective is not subtle.

Berklee budgeted $100,000 for line charges for our fiscal year that began June 1, 2002. This investment represents weekly reinforcement of our motto, providing improved opportunities for our matriculated population as well as new links to Berklee for our alumni and Berklee International Network partner institutions worldwide.

David Lustig is assistant vice president for Information Technology at Berklee. Reach him at dlustig@berklee.edu.

Patricia A. Nelson

Cornell University

ACUTA Ruth A. Michalecki Leadership Award

The ACUTA Ruth A. Michalecki Leadership Award recognizes outstanding leadership among the ACUTA membership. Created in 2001, this award was renamed in 2002 to honor the memory of ACUTA Past President Ruth A. Michalecki, formerly of the University of Nebraska, Lincoln, for her leadership of ACUTA and the telecommunications profession.

Nominees must be ACUTA institutional members, associate members, or corporate affiliates. The person selected for this award:

- Actively participates in and promotes the education, professional development, and mentoring of other professionals.
- Has demonstrated innovation in establishing or changing or has otherwise materially affected the existing practices, usage, and/or concepts applied to the telecommunications profession within higher education (i.e., identifying and advancing telecommunications and/or information technology directions for the benefit of higher education).
- Has engaged in activities that have produced firm and formal results directly benefiting the ACUTA organization and/or the broader higher education community.

In reviewing a list of impressive nominees for this award in 2002, the Awards Committee agreed that Pat Nelson of Cornell University stood out as unquestionably demonstrating the leadership characteristics that this reward was created to recognize.

Pat is a familiar face to ACUTA members, having served the association as president, immediate past president, executive vice president, secretary, Membership Committee chair, and, most recently, Vendor Liaison Committee chair. She has also been a popular presenter at a number of ACUTA events during her 19-year membership.

In 1997, when Pat won the Bill D. Morris Award, then-President Jim Cross called her "a member of many talents, skills, and expertise; a long-term telecommunications professional; a mentor, coach, and leader in the association; a champion of change and strategic planning; a past president; and finally a role model for what outstanding service and commitment means to the association and profession."

Pat has continued to serve and lead in the years since. As director of telecom, assistant director of telecom and networking, deputy director, and now senior business/financial analyst at Cornell, Pat has earned the respect of her colleagues both on campus and within the association. She led her staff through major reorganizations that resulted in higher efficiencies, more client satisfaction, and greater levels of productivity and then shared that process with her peers in ACUTA.

Pat is widely respected as a mentor and role model and is recognized as an innovative thinker and a leader in ACUTA's strategic planning process.

In nominating her for this award, former ACUTA President Margie Milone said, "Pat is the consummate leader. She not only talks the talk, she also walks the walk. She is clearly among the driving force [of those]who have reinvented telephony as a strategic campus service to attract and retain students, faculty, grants, and scholarships through enhanced voice/data/video information technologies deployment and converged operations. By her enormous contributions to the campus telecommunications profession, her personable style of leadership, and her dedication to ACUTA, she exemplifies all the attributes of the ACUTA Ruth A. Michalecki Leadership Award."

Advertisers' Index

★ Indicates ACUTA Corporate Affiliate

By advertising in the *ACUTA Journal,* these companies are not only promoting products and services relevant to telecommunications in higher education, they are also supporting our association. As you have opportunity, we encourage you to mention to these companies that you saw their ad in our journal.

Quotable

In disaster situations, no one, no one at all but you, can be expected to help. You have to be prepared to do it all – with no help. Even if you subcontract to Ma Bell, you are still the person responsible...not Ma Bell. Don't confuse the carrier of 1985 with the carrier of 2003!"

Robert A. O'Neil
O&A Engineering

A disaster recovery plan must be a live plan. It must be exercised, worked, maintained, and tested regularly.

Steve Hailey, project engineer
Daycom Systems

A distributed network focus is better from a survivability and disaster recovery point of view. A centralized network is better from the support and administrative viewpoint. You need to evaluate which is better in your situation.

David Stein
PlanNet Consulting

continued from page 48

mobile and wireless devices make this increasingly true. Campus cultures are antithetical to enforced standards for hardware and software, so the devices and software in use range from the most cutting edge to the most outdated systems. Due to increasingly limited resources and a lack of central authority, some systems are not properly maintained with current anti-virus software and other security measures. The personnel responsible for system maintenance range from students with little or no security training to highly trained technicians.

Campus leaders are recognizing the need for consistent, written goals and policies in the IT security area. Many campuses have created an office of IT security and policy, and have appointed a chief IT security officer. These IT security professionals can be a tremendous resource for ACUTA members as they formulate plans and policies for their own areas, and ACUTA members are also a valuable resource to the campus. I would encourage you to step up to this responsibility, and participate in overall campus IT security planning. Your knowledge of voice, data, and video network issues, your vendor relationships, and your customer relationships with students, faculty, and staff will benefit the overall campus effort.

The participants at the IT Security Summit discussed and endorsed a framework for action that is designed "...to serve as the basis for coordination of a wide variety of activities—at the campus level as well as the national level—...to strengthen the security of higher education information technology systems and resources."[1] The full text of the Framework is available at http://security.internet2.edu/ActionStatement.pdf. The Framework consists of the following elements:

1. Make IT security a higher and more visible priority in higher education.
2. Do a better job with existing security tools, including revision of institutional policies.
3. Design, develop, and deploy improved security for future research and education networks.
4. Raise the level of security collaboration among higher education, industry, and government.
5. Integrate higher-education work on security into the broader national effort to strengthen critical infrastructure.

ACUTA members will be affected by security policies based on new threats, changing laws and regulations, and increased expectations from internal and external sources. I hope that you will be an active participant in the development of policies and procedures on your campus through appropriate channels.

In addition, every ACUTA member will need to be fully aware of how these policies affect your department and personnel and be vigilant in your efforts to safeguard the communications technologies on your campus from security threats.

[1] "Information Technology Critical Infrastructure in Higher Education—A Framework for Action", Security Working Group, EDUCAUSE and UCAID (Internet2). April 2002.

Jeri A. Semer, CAE
ACUTA Executive Director

From the Executive Director

Higher Education Addresses Security Issues

The security of our communications and information systems is one critical component of disaster preparedness and business continuity planning. The higher-education community has, through national associations and prominent higher-education leaders, collectively decided to take an active role in efforts to promote cyber-security and has agreed upon a framework for that effort.

At a series of meetings around the country held in 2002, information-technology experts, institutional and association executives, and government officials addressed issues of cybersecurity as they apply to the higher-education environment. ACUTA participated in the final IT Security Summit in Washington, DC in November 2002. I would like to share some of the highlights of this meeting with you to raise some issues that you may want to consider as you formulate plans for your campus.

Colleges and universities must be particularly conscious of issues including sensitive student information, financial information, medical records, the use of campus IT facilities by persons outside the campus to commit attacks (such as distributed denial-of-service attacks), rapid and wide distribution of viruses, unauthorized access to or tampering with research data, and violation of intellectual property laws. These are in addition to the need to prepare for natural disasters or other emergencies.

As you are aware, the resources at risk include wireless and wired data and voice networks, residence hall facilities, Internet gateways, and Internet2 facilities.

Although the popular press tends to portray campus facilities as "wide open" in their vulnerability to attack or misuse, this is not an accurate characterization. Most campuses implemented appropriate security measures well before the recent high visibility of cybersecurity issues, but recent events have caused every segment of our society to place even more emphasis on the importance of protecting our critical information and infrastructure.

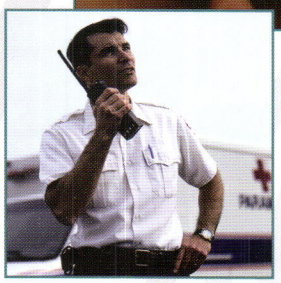
Some of the issues that create unique challenges in the higher-education environment include widely distributed authority and responsibility, the academic culture that encourages access to information and resources, the challenges of the research environment (which involves collaboration among domestic and international institutions), the absence of many clearly defined security goals and policies, and fairly wide access to sensitive data. The age, maturity level, and attitudes of college students are also factors.

In addition, the physical and virtual perimeters of a campus are difficult to define. The escalating presence of distance education, off-campus facilities and partnerships, and

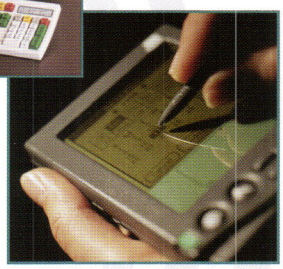
continued on page 47

Cut your costs.
Streamline your communications.
Bring it all together with one system.

Amcom
Comprehensive Call Processing Solutions



- **Speech recognition**
- **PC attendant console**
- **Web-enabled information and services via PC and wireless devices**
- **Enhanced 911 notification**



Never has unified communications been more important to your faculty, administrators and students. Never has it offered greater productivity gains and cost reductions. And never has it been easier to implement and use.

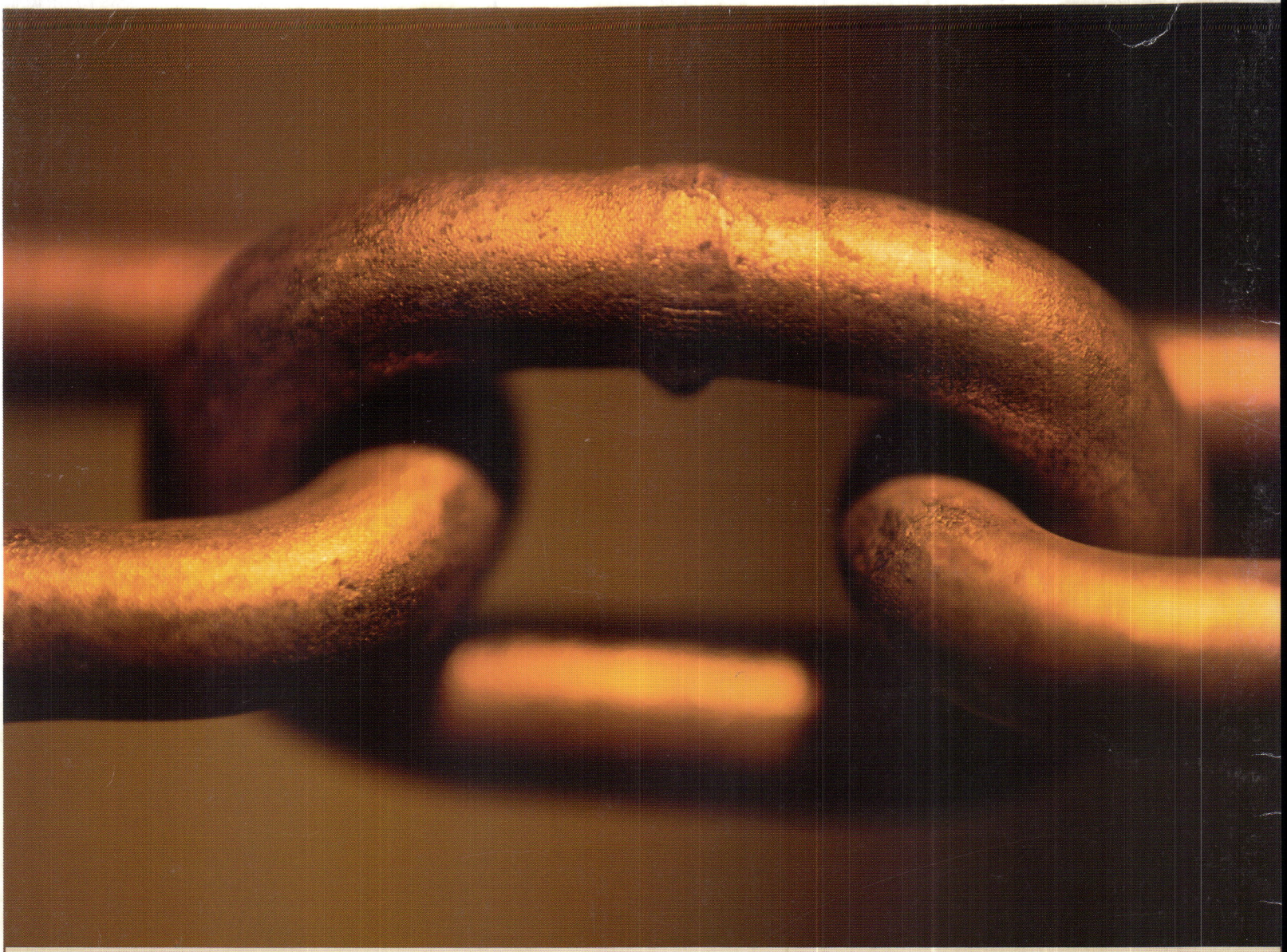
Amcom CTI solutions. Designed with innovation in mind. Built to last using industry-standard hardware, software and protocols.

SERVICES
- Professional system planning and project management
- Turn-key installation and end user training
- 7 x 24 x 365 support

PLATFORMS
Oracle database
Nuance • Intel/Dialogic
Windows NT • Linux

AmCom

1-800-852-8935
www.amcomsoft.com



STRENGTH

THERE'S **STRENGTH** IN OUR 300-PLUS COLLEGE AND UNIVERSITY CUSTOMERS.

PAETEC[SM]
COMMUNICATIONS

For more information, join us at ACUTA, April 27-30, Booth Number 15/16